

**ES GELTEN NUR DIE NACHFOLGEND AUFGEFÜHRTEN SERVICEBESCHREIBUNG(EN)/SLA-ANLAGEN,
DIE DEN UNTER DIESER VEREINBARUNG ERWORBENEN SERVICES ENTSPRECHEN**

ANLAGE 1 DEFINITIONEN UND ALLGEMEINE SERVICEÜBERSICHT

1. Symantec Services

1.1. Symantec liefert jeden über das Internet bereitgestellten und verwalteten Service wie er in den einzelnen Anhängen in Anlage 2, Servicebeschreibungen, definiert ist und mit den entsprechenden Service Level, die in Anlage 3, Service Level Agreement (SLA), definiert sind.

1.2. Jeder Service wird vierundzwanzig (24) Stunden/Tag, sieben (7) Tage/Woche verwaltet. Zum Serviceumfang gehören die Überwachung auf Hardwareverfügbarkeit, Servicekapazität und die Auslastung von Netzwerkressourcen. Jeder Service wird regelmäßig auf die Einhaltung der Service Level überwacht und Anpassungen werden bei Bedarf vorgenommen.

1.3. Für die erfolgreiche Bereitstellung und Leistung des Service sind für jeden Service Informationen vom Kunden erforderlich.

1.4. Der Kunde muss die Verlängerungsidentifikationsdaten, die das Abonnementinstrument (wie unten definiert) begleitet, nach Erhalt auf sein Konto anwenden. Verlängerungsidentifikationsdaten sind erforderlich, um Kontoinformationen und Kundendaten während eines Aufbewahrungszeitraums (falls vorhanden) nach einer Kündigung, wie unten im jeweiligen Serviceanhang festgelegt, weiterzuführen. Andernfalls werden Kontozugriff und Daten ggf. dauerhaft gelöscht.

2. Definitionen

2.1. Die nachfolgenden Begriffe haben im Rahmen dieser Vereinbarung die folgenden Bedeutungen.

"Administrator" bezieht sich auf einen Benutzer im Unternehmen des Kunden, der autorisiert ist, den Service im Auftrag des Kunden zu verwalten. Administratoren können wie vom Kunden festgelegt einen Service komplett oder teilweise verwalten.

"Verbindungsmanager" (Connection Manager) bezeichnet die Erkennungsmethoden, die in der SMTP Handshake-Phase vorhanden sind.

"Gutschriftenantrag" (Credit Request) bezeichnet die Mitteilung, die der Kunde per E-Mail an Symantec an die Adresse support.cloud@symantec.com mit der Betreffzeile "Credit Request" (Gutschriftenantrag) senden muss (sofern nicht anders von Symantec mitgeteilt).

"Ausgewiesener Tower-Cluster" (Designated Tower Cluster) bezeichnet zwei (2) oder mehr Tower, die speziell dafür vorgesehen sind, dem Kunden Email Security Services bereitzustellen.

"Einstellungen für Domänenebene" (Domain Level Settings) bezeichnet Domäneneinstellungen, die für eine bestimmte Domäne in der SMC (Definition siehe weiter unten) für die Email Security Services anpassbar sind.

"Endbenutzer-Lizenzvereinbarung (EULA)" (End User License Agreement (EULA)) bezeichnet die Bedingungen und Bestimmungen, die die Software (Definition siehe weiter unten) begleiten.

"E-Mail" (Email) bezeichnet eine eingehende oder ausgehende SMTP-Nachricht, die über einen Service weitergeleitet wird.

"Email Security Services" sind folgende Services: Email AntiVirus.cloud, Email AntiSpam.cloud, Email Data Protection.cloud, Email Image Control.cloud, Email Boundary Encryption.cloud und Policy Based Encryption.cloud, wie in Anlage 2, Servicebeschreibungen, definiert.

"Email Archiving Services" sind folgende Services: Enterprise Vault.cloud, AdvisorMail on Symantec.cloud, Symantec Email Continuity Archive.cloud, Symantec Email Continuity Archive Lite.cloud, Email Continuity.cloud und Archiving.cloud (P), wie in Anlage 2, Servicebeschreibungen, definiert.

"E-Mail-Virusfehlmeldung" (Email Virus False Positive) bezeichnet eine legitime E-Mail, die fälschlicherweise als vireninfiziert identifiziert wurde.

"Globale Einstellungen" (Global Settings) bezeichnet die Aktionen innerhalb der SMC (Definition siehe weiter unten), die auf alle Domänen und Gruppenebenen für die Email Security Services angewendet werden.

"Einstellungen für Gruppenebene" (Group Level Settings) bezeichnet Gruppeneinstellungen, die für eine bestimmte Gruppe in der SMC (Definition siehe weiter unten) für die Email Security Services anpassbar sind.

"Infrastruktur" (Infrastructure) bezeichnet Technologien und geistiges Eigentum von Symantec oder Lizenzgebern, die für die Bereitstellung der Services genutzt werden.

"Bekannter Virus" (Known Virus) bezeichnet einen Virus, für den zum Zeitpunkt des Eingangs von Content bei Symantec: (i) eine Signatur bereits seit mindestens einer (1) Stunde zur Konfiguration durch Antivirus-Technologie, die von Symantec verwendet wird, öffentlich verfügbar ist; oder (ii) der in der "Wild List" auf <http://www.wildlist.org> enthalten ist und von mindestens zwei Wild List-Teilnehmern als "In the wild" identifiziert wurde.

"Nicht aufteilbares Servicepaket" (Non-Severable Service Bundle) bezeichnet ein aus mehreren Services bestehendes Paket, das in den Tabellen mit aktuellen und älteren nicht aufteilbaren Servicepaketen (Non-Severable Service Bundle and Legacy Name Charts) unter www.symanteccloud.com/documents.aspx aufgeführt ist.

"Mitglied" (Member) bezeichnet den Kunden und Drittparteien, mit denen der Kunde mithilfe des Email Boundary Encryption.cloud Service (Definition siehe weiter unten) ein verschlüsseltes Netzwerk betreibt.

"Monatliche Gebühr" (Monthly Charge) bedeutet die monatliche Gebühr für den (die) in der Vereinbarung aufgeführten Service(s).

"Offener Proxy" (Open Proxy) bezeichnet einen Proxy-Server, der so eingerichtet ist, dass unbekannten oder nicht autorisierten Dritten das Abrufen, Speichern oder Weiterleiten von DNS, Webseiten oder anderen Daten für den Email Security Services ermöglicht wird.

"Open Relay" bezeichnet einen E-Mail-Server, der so konfiguriert ist, dass er E-Mails von nicht bekannten und nicht berechtigten Dritten empfängt und diese E-Mails an einen oder mehrere Empfänger weiterleitet, die nicht Benutzer des E-Mail-Systems sind, an das der E-Mail-Server angebunden ist. Open Relay kann auch als "Spam Relay" oder "Public Relay" bezeichnet werden.

"Servicegutschrift" (Service Credit) bezeichnet den Betrag, der auf der nächsten Rechnung des Kunden gutgeschrieben wird, nachdem er einen Gutschriftenantrag eingereicht hat und von Symantec bestätigt wurde, dass dem Kunden eine Gutschrift zusteht.

"Service Level" bezeichnet die unten in Anlage 3 Service Level Agreement (SLA) definierten Serviceparameter.

"Servicesoftware" (Service Software) bezeichnet Software (Definition siehe weiter unten), die ggf. von einem Service benötigt wird und die auf jedem Kundencomputer installiert sein muss, um den Service zu beziehen. Servicesoftware umfasst die Software und zugehörige Dokumentation, die von Symantec als Teil des Service separat bereitgestellt werden kann.

"Software" bezeichnet ein Softwareprogramm von Symantec oder einem Lizenzgeber in Form von Objektcode, für das Symantec dem Kunden eine Lizenz gewährt und das den Bestimmungen der beiliegenden EULA oder dieser Anlage 1 Definitionen und allgemeine Serviceübersicht unterliegt (wie zutreffend). Die Software umfasst uneingeschränkt neue Versionen oder Updates, die unter dieser Vereinbarung bereitgestellt werden.

"Spam" bezeichnet unerwünschte Werbe-E-Mails.

"Spam False Negative" bezeichnet eine Spam-E-Mail, die nicht vom Email AntiSpam.cloud Service als Spam identifiziert wird.

"Spam False Positive" bezeichnet eine legitime E-Mail, die fälschlicherweise vom Email AntiSpam.cloud Service als Spam identifiziert wird.

"Empfohlene Spam-Einstellungen" (Spam Recommended Settings) bezeichnet die Symantec-Richtlinie mit empfohlenen Konfigurationseinstellungen für den Email AntiSpam.cloud Service, die dem Kunden während des Bereitstellungsprozesses ausgehändigt wird oder wie in der Online-Hilfe veröffentlicht.

"Abonnementinstrument" (Subscription Instrument) bezieht sich auf eines oder mehrere der zugehörigen Dokumente, die die Rechte und Pflichten des Kunden in Bezug auf den Service näher definieren: ein Symantec-Zertifikat bzw. ein vergleichbares von Symantec ausgestelltes Dokument oder eine schriftliche Vereinbarung zwischen dem Kunden und Symantec, das/die den Service begleiten, ihm vorausgehen oder nachfolgen.

"Symantec Tracker" bezeichnet ein Tool von Symantec, mit dem die Serviceverfügbarkeit und Latenz wie in Anlage 3, Service Level Agreement (SLA), für die Email Security Services gemessen werden.

"Tower" bezeichnet einen Cluster aus E-Mail-Servern mit Lastverteilung.

"Unbekannter Virus" (Unknown Virus) bezeichnet einen Virus, für den zum Zeitpunkt des Eingangs von Content bei Symantec: (i) eine Signatur noch nicht seit mindestens einer (1) Stunde zur Konfiguration durch Antivirus-Technologie, die von Symantec verwendet wird, öffentlich verfügbar ist; oder (ii) der nicht in der "Wild List" auf <http://www.wildlist.org> enthalten ist und von mindestens zwei Wild List-Teilnehmern als "In the wild" identifiziert wurde.

"Benutzer" bezeichnet eine Einzelperson und/oder ein Gerät, die/das autorisiert ist, den Service zu nutzen und/oder von der Nutzung des Service profitieren bzw. die/das effektiv einen Teil des Service nutzt. Für die Email Security Services und/oder Email Archiving Services schließt die Definition von **"Benutzer"** sämtliche Postfächer ein, die E-Mails senden und/oder empfangen.

"Virus" bezeichnet Programmcode, einschließlich eines sich selbst vervielfältigenden Bestandteils, der sich in der Regel als etwas anderes tarnt und so programmiert ist, dass er andere Computersysteme infizieren kann.

"Massen-E-Mails" bezeichnet ein Paket von mehr als fünftausend (5.000) E-Mail-Nachrichten (die von einem Kunden gesendet oder empfangen werden) mit überwiegend gleichem Inhalt, die in einem Vorgang oder in einer Reihe zusammenhängender Vorgänge an Einzelpersonen oder eine Verteilerliste versendet werden, wie etwa Marketingmaterial, Warnmeldungen, Newsletter oder andere Formen der Massenkommunikation.

"Web Services" bezeichnet zusammenfassend die Web v2 Protect.cloud und Web v2 URL.cloud Services.

3. Service Management Console (SMC)

3.1. Jede Service Management Console (wie zutreffend) ist eine Online-Ressource und ein internetbasiertes Tool, das dem Kunden als Teil eines Service zur Verfügung gestellt wird. Der Kunde kann mithilfe sicherer, kennwortgeschützter Zugangsdaten auf die SMC zugreifen. Über die SMC kann der Kunde den Service konfigurieren und verwalten, Berichte abrufen sowie Daten und Statistiken anzeigen, wenn diese als Teil des Service bereitgestellt werden. Ein Kunde kann Zugriff auf mehrere SMCs erhalten, um verschiedene Services zu verwalten (z. B. ClientNet, CMES oder Manage).

4. Übersicht über die Email Security Services

4.1. Die Email Security Services stehen nur Kunden zu Verfügung, die über einen eigenen E-Mail-Domännennamen verfügen und die MX-Einträge und/oder DNS für diesen Domännennamen konfigurieren können.

4.2. Der Kunde muss seine eingehenden E-Mails mithilfe der MX-Einträge, die er zum Zeitpunkt der Servicebereitstellung angegeben hat, an Symantec weiterleiten. Der Kunde kann optional seine ausgehenden E-Mails über Symantec weiterleiten, um sämtliche Vorteile der Email AntiVirus.cloud, Email Data Protection.cloud und Email Image Control.cloud Services zu nutzen. Policy Based Encryption.cloud setzt voraus, dass der Kunde seine ausgehenden E-Mails über Symantec weiterleitet. Der Kunde sollte E-Mails nicht an einen bestimmten Tower oder eine bestimmte E-Mail-Adresse weiterleiten. Um Missverständnisse auszuschließen: Anlage 3, Service Level Agreement (SLA), gilt nicht für Domänen, die nicht in Übereinstimmung mit dieser Klausel bereitgestellt werden.

4.3. Für die erfolgreiche Ausführung der Email Security Services muss der Kunde sicherstellen, dass Domänen (einschließlich Sub-Domänen) in der jeweiligen Serviceinfrastruktur bereitgestellt werden und der jeweilige Service für diese Domänen abonniert ist, wie im entsprechenden Anhang in Anlage 2, Servicebeschreibung, beschrieben. Der Kunde akzeptiert, dass die Servicefunktionen ggf. nicht korrekt funktionieren und die E-Mail-Zustellung für Domänen, die nicht entsprechend bereitgestellt werden, nicht möglich ist. Um Missverständnisse auszuschließen: Anlage 3, Service Level Agreement (SLA), gilt nicht für Domänen, die nicht in Übereinstimmung mit dieser Klausel bereitgestellt werden.

4.4. Der Kunde muss sicherstellen, dass er eingehende E-Mails nur aus der Symantec Email Security Services-Infrastruktur akzeptiert. Um Missverständnisse auszuschließen: Service Level Agreements gelten nur für eingehende E-Mails, die von den Symantec Email Security Services gescannt wurden.

4.5. Der Kunde muss eingehende E-Mails von allen von Symantec geforderten IP-Bereichen akzeptieren, um eine kontinuierliche Serviceverfügbarkeit sicherzustellen, falls ein Teil der Infrastruktur nicht verfügbar ist. Um Missverständnisse auszuschließen: Service Level Agreements gelten nur für E-Mails, die von den Symantec Email Security Services gescannt wurden.

4.6. Für alle eingehenden E-Mails wird die IP-Reputation des Absenders mithilfe verfügbarer Informationsquellen ermittelt. E-Mails aus einer unseriösen Quelle (z. B. von einem Spammer) werden verzögert, um die Auswirkungen auf die Netzwerkapazität zu reduzieren.

4.7. Um eine kontinuierliche Serviceverfügbarkeit bereitzustellen, gilt Folgendes: Falls sich ein Kunde entscheidet, ausgehende E-Mails durch den Email Security Service zu leiten, behält sich Symantec das Recht vor, sämtliche E-Mails wie z. B. Spam auf bösartigen Content zu scannen. Ausgehende E-Mails, die spamverdächtig sind, werden vom Email Security Service nicht akzeptiert. Wird eine ausgehende E-Mail als spamverdächtig erkannt, wird eine Meldung über einen permanenten SMTP-Fehler (5xx) an den MTA des Kunden ausgegeben. Die meisten MTAs erzeugen daraufhin standardmäßig eine Unzustellbarkeitsmeldung (Non Delivery Receipt, NDR), um den Absender über die 5xx-Fehlermeldung zu informieren. Ausgehende E-Mails, die spamverdächtig sind, werden nicht in den in der SMC erstellten Email Security Service-Berichten erfasst. In Track and Trace (wie unten definiert) wird angezeigt, dass eine ausgehende E-Mail als Spam erkannt und nicht akzeptiert wurde. Die Service Level für die Spam-Erfassungsrates und Spam False Positives (Spam-Fehlermeldungen) gelten nicht für ausgehende E-Mails. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE SPAM NICHT ERKENNT ODER LEGITIME E-MAIL FÄLSCHLICHERWEISE ALS SPAM IDENTIFIZIERT.

4.8. Kunden, die Email Security Services nutzen, müssen die Mail-Server-IP-Adresse(n) oder -Hostnamen für die Zustellung eingehender E-Mails an ihr Unternehmen angeben. Zudem können sie in der SMC Zustellungskanäle für eingehende E-Mails entweder für alle bereitgestellten Domänen oder nur für bestimmte Domänen festlegen. Ferner kann der Kunde "Pro-Benutzer-Routing" anfordern, um eingehende E-Mails für bestimmte Benutzer an eine Mail-Server-IP-Adresse weiterzuleiten. Die Aktivierung dieser Funktion unterliegt dem alleinigen Ermessen von Symantec. Kunden, die die "Pro-Benutzer-Routing"-Funktion nutzen, sind alleinig für die Bereitstellung und Wartung der Konfigurationsdateien, wie im von Symantec bereitgestellten "Per User Routing Administration Guide" beschrieben, verantwortlich. DER KUNDE STIMMT ZU, DASS SYMANTEC KEINE HAFTUNG FÜR DIE NICHTZUSTELLUNG ODER FEHLZUSTELLUNG VON E-MAILS ÜBERNIMMT, DIE AUFGRUND VON FEHLERN ODER AUSLASSUNGEN IN DEN "PRO-BENUTZER-ROUTING"-KONFIGURATIONSDATEIEN ENTSTEHEN. Die Bereitstellung der "Pro-Benutzer-Routing"-Funktion kann länger dauern als die Bereitstellung anderer Services. Klausel 8.2 weiter unten findet daher keine Anwendung.

4.9. Symantec wird versuchen, E-Mails an die konfigurierten eingehenden IP-Adressen oder Hostnamen des Kunden (wie in der SMC konfiguriert) wiederholt für einen Zeitraum von bis zu sieben (7) Kalendertagen zuzustellen. Der Absender wird benachrichtigt, falls die E-Mail nicht zugestellt werden konnte. Danach werden nicht zugestellte E-Mails aus der Warteschlange gelöscht.

4.10. Die maximal zulässige E-Mail-Größe für die Email Security Services beträgt 50 MB. Der Kunde kann eine maximale E-Mail-Größe in der SMC festlegen. E-Mails, die von dem jeweiligen Service empfangen werden und die festgelegte Höchstgrenze überschreiten, werden blockiert und gelöscht. Eine Benachrichtigung wird an den Absender, den vorgesehenen Empfänger und einen Administrator gesendet.

4.11. Der Kunde erklärt sich einverstanden, eine Liste einzelner E-Mail-Adressen, auf die der Service anzuwenden ist, zur Verfügung zu stellen und zu verwalten ("**Validierungsliste**"). Der Kunde ist dafür verantwortlich, diese Validierungsliste vor der Bereitstellung des Service und während der Laufzeit der Vereinbarung zu überprüfen. Der Kunde erkennt an, dass eingehende E-Mails, die an E-Mail-Adressen gerichtet sind, welche nicht oder fehlerhaft in der Validierungsliste eingetragen sind, automatisch blockiert werden. Der Kunde stimmt zu, dass Symantec nicht haftbar ist, wenn E-Mails aufgrund von Fehlern oder Auslassungen in der Validierungsliste nicht zugestellt werden können.

4.12. Der Kunde verpflichtet sich, nicht zuzulassen, dass seine Systeme: (i) als Open Relay oder Open Proxy fungieren; (ii) Massen-E-Mails senden oder empfangen, die vom Kunden stammen, es sei denn, der Kunde hat den Volume Mail Service (wie unten definiert) abonniert; in diesem Fall ist der Kunde berechtigt, Massen-E-Mail unter strikter Einhaltung der für diesen Service geltenden Bestimmungen zu versenden und zu empfangen; oder (iii) Spam versenden. Symantec behält sich das Recht vor, die Einhaltung dieser Klausel durch den Kunden von Zeit zu Zeit zu überprüfen. Um Missverständnisse auszuschließen: Ein Verstoß gegen diese Klausel wird als ein wesentlicher Verstoß gegen diese Vereinbarung betrachtet. Symantec behält sich das Recht vor, die Bereitstellung des Service ganz oder teilweise mit sofortiger Wirkung und bis zur Behebung des Verstoßes auszusetzen oder die Vereinbarung für den betroffenen Email Security Service zu kündigen.

4.13. Der Kunde kann einen Haftungsausschlusstext konfigurieren, der an jede eingehende und ausgehende E-Mail, die von den Symantec Email Security Services gescannt wird, angefügt wird. Ab dem Zeitpunkt der Servicebereitstellung wird ein Standard-Haftungsausschluss übernommen, dessen Inhalt vom Kunden in der SMC bearbeitet werden kann. Der Kunde kann unterschiedliche Haftungsausschlusstexte für eingehende E-Mails und ausgehende E-Mails konfigurieren. Diese können allen E-Mails oder bestimmten Domänen und Benutzergruppen zugewiesen werden. Haftungsausschlusstexte können nur von SMC-Benutzern mit der Berechtigung zur Konfigurationsänderung für alle in dem Konto bereitgestellten Domänen konfiguriert werden.

4.14. Track and Trace. Symantec bietet die Möglichkeit, Nachrichten in der SMC nachzuverfolgen. Der Kunde kann so nach einer bestimmten E-Mail suchen und feststellen, ob und wann der Email Security Service die Nachricht verarbeitet hat und welche Aktion durchgeführt wurde. E-Mails stehen innerhalb von 15 Minuten, nachdem sie in der Email Security Services-Infrastruktur akzeptiert wurden, für die Suche zur Verfügung und bleiben dreißig (30) Kalendertage für Suchvorgänge aktiviert. Die Email Security Services speichern keine Kopien von E-Mails, die die Infrastruktur durchlaufen. Track and Trace wird als Problemlösungstool zur Verfügung gestellt, mit dem sich bestimmte E-Mails nachverfolgen lassen. Es ist kein Tool für die Berichterstattung. Die Anzahl der Ergebnisse, die von einem Suchlauf ausgegeben werden können, ist begrenzt. Nur SMC-Benutzer mit den entsprechenden Berechtigungen können auf Track and Trace zugreifen. Ein Administrator kann einzelnen Portalbenutzern eine Track and Trace-Benutzerrolle zuweisen. Der Zugriff auf Track and Trace ist für alle Domänen möglich, die für das Konto des Kunden bereitgestellt wurden.

4.15. Mit der End User Email Quarantine ("Spam Manager"), falls diese vom Kunden angefordert und von Symantec aktiviert wurde, können Benutzer E-Mails verwalten, die vom Email AntiSpam.cloud Service isoliert wurden. Benutzer können E-Mails löschen oder in einem vom Benutzer ausgewählten E-Mail-Posteingang freigeben. Benutzer können festlegen, ob der Textinhalt dieser E-Mails angezeigt werden kann. Isolierte E-Mails können von einzelnen Benutzern oder von anderen ausgewählten Personen verwaltet werden. Benutzer können festlegen, dass sie regelmäßig Benachrichtigungen erhalten, wenn E-Mail vom Service isoliert wird. Isolierte E-Mails werden vierzehn (14) Kalendertage lang gespeichert und danach automatisch gelöscht. Benutzer können diese E-Mails innerhalb dieser Frist ohne Einschränkungen anzeigen. Der Kunde kann die Speicherdauer bei Bedarf gegen eine zusätzliche Gebühr verlängern. In dem seltenen Fall, dass das User Quarantine-System keine E-Mails annehmen kann, werden die E-Mails so lange gespeichert, bis das End User Email Quarantine-System wieder funktionsfähig ist. Danach kann wieder über das Quarantine-System auf die E-Mails zugegriffen werden. Falls die Benachrichtigungsfunktion aktiviert ist, sind sie in der nächsten Übersichtsbenachrichtigung aufgeführt.

4.16. Der Kunde kann die alternative Email Quarantine ("Message Manager") anfordern. Symantec wird diese Anfrage im Einzelfall prüfen und behält sich das Recht vor, nach alleinigem Ermessen die Aktivierung des Message Manager für einen Kunden abzulehnen. Mithilfe des Message Manager können Benutzer bestimmte Funktionen für die Verwaltung von E-Mails nutzen, die von den Email AntiSpam.cloud-, Email Image Control.cloud- und Email Data Protection.cloud-Services isoliert wurden. Die aktuelle Version des Message Manager ist eine Version mit eingeschränkter Verfügbarkeit und wird Kunden "wie geliefert" bereitgestellt. Es unterliegt der alleinigen Verantwortung des Kunden, zu prüfen, dass die Funktionalität des Message Manager seinen Ansprüchen genügt, bevor er eine Anfrage für die Bereitstellung des Service an Symantec sendet. E-Mails können maximal vierzehn (14) Tage in Message Manager gespeichert werden. Nach dieser Frist werden sie automatisch gelöscht. Quarantine-Speicherung mithilfe von Message Manager ist auf 5 MB pro Benutzer beschränkt, wobei dieser Wert aus dem Mittelwert für sämtliche Benutzer des Kunden errechnet wird. Symantec überwacht die Nutzung. Falls das Kontingent des Kunden überschritten wird, kann Symantec Nachrichten löschen oder eine Benachrichtigung an die Empfänger bzw. an den Administrator senden. SYMANTEC SCHLIESST JEGLICHE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN ZUSICHERUNGEN, BEDINGUNGEN ODER GEWÄHRLEISTUNGEN IN BEZUG AUF DEN MESSAGE MANAGER AUS. Anlage 3, Service Level Agreement (SLA), gilt nicht für Message Manager.

5. Berichterstattung

5.1. Die Berichterstattung für jeden Service erfolgt über die für diesen Service verwendete SMC und wie unten in Anlage 2 Servicebeschreibungen, definiert.

5.2. Die Berichterstattung zu Aktivitäten der Email Security Services, der Web Services und des Instant Messaging Security.cloud Service (wie unten definiert) sowie Statistiken sind über die SMC verfügbar. Der Kunde kann die SMC so konfigurieren, dass Berichte erstellt werden, die nach einem bestimmten Zeitplan per E-Mail an den Kunden versendet werden oder von der SMC heruntergeladen werden können.

6. Geplante Wartung

6.1. "**Geplante Wartung**" bezieht sich auf Wartungsintervalle, die Symantec dem Kunden sieben (7) Tage vor Durchführung durch Veröffentlichung in der SMC mitteilt und die zu einer Beeinträchtigung des Services mangels Verfügbarkeit der Serviceinfrastruktur führen können. Symantec unternimmt alle wirtschaftlich vertretbaren Anstrengungen, um die geplante Wartung nicht Montag bis Freitag zwischen 8.00 Uhr und 18.00 Uhr (in der Zeitzone, in der sich die Infrastruktur befindet) durchzuführen.

6.2. Soweit möglich, wird die geplante Wartung ohne Beeinträchtigung des Service erbracht. Die geplante Wartung wird in der Regel während Zeiten mit erwartungsgemäß geringem Datenverkehr und nur für einzelne Teile des Netzwerks und nicht für das gesamte Netzwerk durchgeführt. Während der Durchführung der geplanten Wartung wird der Service über solche Teile des Netzwerks umgeleitet, die nicht gewartet werden, um die Beeinträchtigung des Service gering zu halten.

6.3. Werden Notfallwartungsarbeiten notwendig und ist wahrscheinlich, dass hierdurch der Service beeinträchtigt wird, wird sich Symantec bemühen, die betroffenen Parteien zu informieren, und eine Warnmeldung in der jeweiligen SMC innerhalb einer (1) Stunde nach Beginn der Notfallwartungsarbeiten veröffentlichen.

6.4. Die routinemäßige Wartung der SMC wird außerhalb von Spitzenbelastungszeiten ausgeführt, um die Verfügbarkeit der SMC so wenig wie möglich zu beeinträchtigen. Symantec unternimmt alle wirtschaftlich vertretbaren Anstrengungen, um diese Wartungsintervalle auf maximal dreißig (30) Minuten zu beschränken. Der Kunde wird vorab nicht über diese Wartungsarbeiten unterrichtet.

7. Technischer Support

7.1. Technischer Support wird vierundzwanzig (24) Stunden/Tag und sieben (7) Tage/Woche geleistet, um dem Kunden bei der Konfiguration der in den entsprechenden Anhängen beschriebenen Servicefunktionen zu unterstützen und um Probleme mit dem Service zu lösen. Weitere Informationen zum technischen Support können unten in Anlage 2, Servicebeschreibungen, aufgeführt sein.

8. Kundenservice

8.1. Symantec wird seinen Kundenservice innerhalb der örtlichen Geschäftszeiten von Symantec wie folgt erbringen:

- a) um Aufträge hinsichtlich der Bereitstellung des Service entgegenzunehmen und zu bearbeiten
- b) um Anfragen zur Änderung betrieblicher Aspekte des Service entgegenzunehmen und zu bearbeiten, und
- c) um auf Fragen im Zusammenhang mit Rechnungen und Zahlungen einzugehen

8.2. Wenn nicht anders im jeweiligen Anhang angegeben, unternimmt Symantec nach Erhalt einer vollständig ausgefüllten und gültigen Bestellung oder Serviceänderungsanfrage alle wirtschaftlich vertretbaren Anstrengungen, um den Service innerhalb von fünf (5) Werktagen bereitzustellen, vorausgesetzt, der Kunde hat alle erforderlichen Informationen an Symantec weitergeleitet.

9. Lizenz für Servicesoftware

Für jeden Service, für den dem Kunden Servicesoftware bereitgestellt wird, gilt die EULA, die der Servicesoftware beiliegt. Falls der Servicesoftware keine EULA beiliegt, gelten die nachfolgenden Bestimmungen. Diese Klausel 9 gilt nicht für Software, die dem Kunden als Teil einer vor Ort installierten Option bereitgestellt wird, falls ein Service die Auswahl zwischen einer Cloud-verwalteten oder vor Ort installierten Lösung vorsieht.

9.1. **Lizenzgewährung.** Vorbehaltlich der Bestimmungen und Bedingungen dieser Vereinbarung gewährt Symantec dem Kunden das nicht ausschließliche, nicht übertragbare Recht zur Installation und Nutzung der Servicesoftware und nur soweit dies für den internen Unternehmensbetrieb des Kunden erforderlich ist. Alle Rechte am geistigen Eigentum in der Servicesoftware sind und bleiben im Besitz von Symantec und/oder deren Zulieferer. Die Servicesoftware wird nicht verkauft, sondern von Symantec lizenziert. Der Kunde bestätigt, dass die Servicesoftware und sämtliche zugehörigen Informationen, einschließlich und uneingeschränkt aller Updates, Eigentum von Symantec und deren Zulieferern ist. Der Kunde übernimmt die Verantwortung und haftet

uneingeschränkt für die Einhaltung oder die Verletzung der Bestimmungen dieser Vereinbarung durch jeden einzelnen Benutzer. Der Kunde verpflichtet sich, Symantec umgehend über jede nicht autorisierte Nutzung oder einen Verstoß gegen diese Bestimmungen zu informieren.

9.2. Kopier- und Nutzungseinschränkungen. Der Kunde darf die Servicesoftware unter den folgenden Bedingungen herunterladen und installieren:

- a) Der Kunde darf die Servicesoftware maximal für die Anzahl der Endbenutzerlizenzen, für die der Kunde eine Lizenz erhalten hat, herunterladen oder installieren.
- b) Der Kunde darf die Servicesoftware, soweit dies billigerweise erforderlich ist, zu Zwecken der Datensicherung, der Archivierung oder der Notfallwiederherstellung (Disaster Recovery) kopieren. Gedruckte Dokumentation darf vom Kunden nur für den internen Gebrauch vervielfältigt werden. "**Dokumentation**" bezeichnet in der heruntergeladenen Servicesoftware enthaltene Benutzerhandbücher und/oder Handbücher zur Bedienung der Software von Symantec.
- c) Der Kunde ist nicht berechtigt und hat auch nicht das Recht, einer Drittpartei zu gestatten: (i) die Servicesoftware ohne vorherige schriftliche Genehmigung von Symantec zu dekompile, zu disassemblieren oder zurückzuentwickeln (reverse engineering), soweit dies nicht nach geltendem Recht ausdrücklich zulässig ist; (ii) Produktkennzeichnungen oder Hinweise auf Eigentumsrechte zu entfernen; (iii) die Servicesoftware zu vermieten, zu verleihen oder zu Timesharing- oder Servicebüro-Zwecken zu nutzen; (iv) die Servicesoftware zu verändern, zu übersetzen, anzupassen oder abgeleitete Produkte davon zu erstellen; oder (v) die Servicesoftware in anderer Weise zu nutzen oder zu kopieren, soweit dies hierin nicht ausdrücklich vorgesehen ist.

9.3. Übertragung von Rechten. Der Kunde darf diese Lizenz aus dieser Vereinbarung ohne vorherige schriftliche Zustimmung von Symantec nicht übertragen, abtreten oder weitergeben. Jegliche Übertragung, Abtretung oder Weitergabe entgegen dieser Bestimmung ist nichtig.

9.4. Beschränkte Gewährleistung und Haftungsausschluss

- a) Symantec gewährleistet, dass nach dem Herunterladen die Servicesoftware in allen wesentlichen Belangen der aktuellen Dokumentation von Symantec entspricht.
- b) Die vorstehende Gewährleistung gilt nicht, wenn: (i) die Software nicht gemäß dieser Vereinbarung oder der Dokumentation genutzt wird; (ii) die Servicesoftware oder Teile davon durch einen anderen Rechtsträger als durch Symantec verändert wurden; oder (iii) eine Fehlfunktion in der Servicesoftware durch Anlagen oder Geräte des Kunden oder durch fremde Software verursacht wurde.
- c) SYMANTEC GEWÄHRLEISTET NICHT, DASS DER BETRIEB DER SOFTWARE UNUNTERBROCHEN ODER FEHLERFREI IST. Symantec schließt jegliche ausdrücklichen oder stillschweigenden Gewährleistungen aus, einschließlich, aber nicht darauf beschränkt, der stillschweigenden Garantien der Veräußerlichkeit, der zufriedenstellenden Qualität oder der Eignung für einen bestimmten Zweck.

9.5. Kündigung. Mit Kündigung des jeweiligen Service oder der Vereinbarung enden mit sofortiger Wirkung alle hierin gewährten Rechte des Kunden zur Nutzung der Servicesoftware; der Kunde muss alle Kopien der Servicesoftware und der Dokumentation umgehend an Symantec zurückgeben oder vernichten.

10. Synchronisierungstools und APIs

10.1. Schemus-Tool. Das Schemus-Tool ist eine Software, die Daten zwischen dem Verzeichnisserver des Kunden und bestimmten Symantec-Services synchronisiert. Die Lizenz für das Schemus-Tool wird dem Kunden von Schemus Limited im Rahmen der EULA, die den Download des Schemus-Tools begleitet, erteilt. Der Kunde bestätigt und erkennt an, dass der Zugriff auf das Schemus-Tool und dessen Nutzung davon abhängig sind, dass der Kunde die Bestimmungen der EULA von Schemus Limited akzeptiert und einhält. Eine Kopie der EULA ist auf Anfrage bei Symantec erhältlich. Symantec gibt keine weiteren (ausdrücklichen, stillschweigenden, gesetzlichen oder sonstigen) Garantien in Bezug auf das Schemus-Tool ab. Falls ein Defekt im Zusammenhang mit den drei (3) neuesten Versionen des Schemus-Tools auftritt, unternimmt Symantec wirtschaftlich angemessene Anstrengungen, um die Problemquelle zu ermitteln und das Problem gegebenenfalls an Schemus Limited zu eskalieren. Symantec wird alle wirtschaftlich angemessenen Anstrengungen unternehmen, um den Kunden dreißig (30) Kalendertage im Voraus über die SMC oder per E-Mail darüber zu informieren, ob Symantec die Nutzung und/oder die Unterstützung des Schemus-Tools und der zugehörigen API einstellen wird. Falls verfügbar, erhält der Kunden gleichzeitig Informationen über ein alternatives Synchronisierungstool. DER KUNDE STIMMT ZU, DASS DIE HÖCHSTHAFTUNG VON SYMANTEC GEGENÜBER DEM KUNDEN IN BEZUG AUF DAS SCHEMUS-TOOL AUF EINE SUMME ENTSPRECHEND DEM VOM KUNDEN AN SYMANTEC FÜR DAS SCHEMUS-TOOL TATSÄCHLICH GEZAHLTEN BETRAG ODER EINEN BETRAG VON

500 US-DOLLAR BEGRENZT IST, WOBEI DER HÖHERE BETRAG DER JEWEILS MASSGEBLICHE BETRAG IST.

10.2. Enterprise Vault.cloud CloudLink Option. Die CloudLink Option ist eine Software, die Daten zwischen dem Verzeichnisserver des Kunden und bestimmten Symantec-Services synchronisiert. Die CloudLink Option wird dem Kunden im Rahmen der oben beschriebenen Lizenz für die Servicesoftware lizenziert.

11. Zusätzliche rechtliche Bestimmungen und Bedingungen

Die folgenden Bestimmungen gelten für alle Services. Der Kunde akzeptiert und stimmt zu, dass:

11.1. Jeder Service dafür vorgesehen ist, dem Kunden die Möglichkeit zu geben, eine gültige und durchsetzbare Computernutzungsrichtlinie (oder deren Entsprechung) zu implementieren. Der Kunde verpflichtet sich, sämtliche geltenden Gesetze in Bezug auf die Nutzung des Service/der Services einzuhalten. In bestimmten Ländern muss gegebenenfalls die Zustimmung einzelner Mitarbeiter eingeholt werden. Die Konfiguration und Nutzung der Services unterliegt vollständig der Kontrolle des Kunden. Symantec ist nicht für die Nutzung der Software durch den Kunden haftbar und übernimmt auch keine Verantwortung für die zivilrechtliche oder strafrechtliche Haftung, die der Betrieb des Service durch den Kunden nach sich ziehen kann.

11.2. Alle von Symantec zur Verfügung gestellten Vorlagen erfüllen nur die Funktion von Richtvorlagen, anhand derer der Kunde seine eigenen, individuell angepassten Richtlinien und andere Vorlagen erstellen kann.

11.3. Vorgeschlagene Wortlisten und Vorlagenregeln oder -richtlinien, die Symantec zur Verfügung stellt, können Wörter enthalten, die als beleidigend betrachtet werden.

11.4. Der Kunde ist nicht berechtigt, ohne vorherige schriftliche Genehmigung von Symantec die Ergebnisse von Benchmark-Tests oder anderen Tests im Zusammenhang mit dem Service einer Drittpartei gegenüber offenzulegen.

11.5. Für den Fall, dass die fortlaufende Bereitstellung der Software für den Kunden die Sicherheit des Service beeinträchtigt, einschließlich, ohne darauf beschränkt zu sein, Hacker-Angriffe, Denial-of-Service-Angriffe, Mail-Bomben oder andere bösartige Aktivitäten, die an die Domänen des Kunden gerichtet sind oder von dessen Domänen ausgehen, stimmt der Kunde zu, dass Symantec den Service für den Kunden vorübergehend aussetzen kann. In einem solchen Fall wird Symantec den Kunden umgehend informieren und mit dem Kunden zusammenarbeiten, um diese Probleme zu lösen. Sobald die Sicherheitsbedrohung beseitigt ist, wird Symantec den Servicebetrieb wieder aufnehmen.

11.6. Sollte ein Service aus irgendeinem Grund ausgesetzt oder beendet werden, macht Symantec sämtliche Konfigurationsänderungen, die nach der Bereitstellung des Service vorgenommen wurden, rückgängig. Der Kunde ist dafür verantwortlich, alle notwendigen Konfigurationsänderungen vorzunehmen, sobald der Servicebetrieb wieder aufgenommen wird.

11.7. E-Mails, Instant Messages, Webseiten oder ihre Anhänge werden von Symantec nicht auf irgendeine andere Weise als mit elektronischen Mitteln abgerufen, gelesen oder kopiert, soweit dies zu Zwecken der Servicebereitstellung erforderlich ist. Symantec behält sich jedoch das Recht vor, Inhalte im Zusammenhang mit Viren, Spam, Malware, Adware und Spyware in diesen E-Mails, Instant Messages, Webseiten und ihren Anhängen für diese alleinigen Zwecke zu nutzen: (i) um die Leistung des Service aufrechtzuerhalten und zu verbessern; und (ii) um den Lizenzgebern des Service Informationen bereitzustellen, die durch den Service fließen, die für die Lizenzgeber zu dem alleinigen Zweck von Interesse sind, um den Service weiterzuentwickeln und zu optimieren. Falls Symantec die unter dieser Klausel eingeräumten Rechte wahrnimmt, wird Symantec alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um alle Informationen, die Symantec vom Kunden erhält oder die Symantec im Zusammenhang mit diesem Service an den Kunden sendet, vertraulich zu behandeln.

11.8. Service Level gelten für die unten in Anlage 3, Service Level Agreement (SLA) beschriebenen Services sowie für jeden Vorgängerservice (falls zutreffend).

11.9. Symantec stellt dem Kunden eine Einrichtungsgebühr zu den dann geltenden Preisen in Rechnung (falls zutreffend), wenn der Kunde die Anzahl der Benutzer erhöht oder den Service/die Services in einer Weise nutzt, die über die vereinbarte Nutzung hinausgeht.

11.10. Die registrierte Nutzung kann nur in Intervallen von zehn (10) Benutzern erhöht werden.

11.11. Zur Optimierung des jeweiligen Service kann Symantec nach eigenem Ermessen jederzeit und ohne vorherige Ankündigung Funktionen zu jedem Service hinzufügen oder Servicefunktionen ändern bzw. entfernen. Symantec ist berechtigt, nach eigenem Ermessen gelegentlich allgemeine Betriebspraktiken aufzustellen oder abzuändern, um den Betrieb und die Verfügbarkeit des Service zu optimieren und Missbrauch zu verhindern.

Um Missverständnisse auszuschließen: Diese Änderungen führen nicht zu einer wesentlichen Verschlechterung der Qualität des Service.

Symantec kann diese Servicebeschreibungen von Zeit zu Zeit aktualisieren, um den bereitgestellten Service adäquat zu beschreiben.

11.12. Der Kunde erkennt an und stimmt zu, dass die in dieser Vereinbarung beschriebenen Rechtsbehelfe den einzigen und ausschließlichen Rechtsbehelf darstellen, falls ein Service nicht die in dieser Vereinbarung festgelegten Leistungen erbringt.

11.13. Jeder Service und jede damit bereitgestellte Servicesoftware nutzt gegebenenfalls Open Source-Code und anderes Material von Dritten. Diese unterliegen einer separaten Lizenz. Weitere Informationen dazu erhalten Sie in dem jeweiligen Hinweis zu Drittanbietern unter

<http://www.symantec.com/about/profile/policies/eulas/>.

12. Kündbarer ("Opt-Out") Verlängerungsprozess

Der Service wird wie in der Vereinbarung, die auf diese Servicebeschreibungen verweist, beschrieben automatisch verlängert, es sei denn, eine solche Verlängerung wird wie folgt gekündigt:

12.1. Der Kunde kann die automatische Verlängerung für die Services in den Anhängen 1 bis 20 dieser Servicebeschreibungen kündigen, indem er Symantec bis spätestens drei (3) Monate vor der zu diesem Zeitpunkt gültigen Mindestlaufzeit oder Verlängerungslaufzeit des Kunden (beides eine "Laufzeit") unterrichtet. Diese Mitteilung über die Kündigung ist vom Kunden per E-Mail an folgende Adresse zu senden:

CLD_cancellations_MLABS@symantec.com, entweder direkt oder über den autorisierten Vertriebspartner des Kunden. Eine Mitteilung über die Kündigung der Verlängerung wird nach Ablauf der dann gültigen Laufzeit wirksam. Sämtliche Mitteilungen über Kündigungen, die wie in dem oben beschriebenen Verfahren an Symantec erfolgen, gelten als eingereicht, wenn sie bei Symantec eingehen. Die Kündigung aller anderen Services hat nach dem Verfahren zu erfolgen, das in dem jeweiligen Anhang der Servicebeschreibungen beschrieben ist.

**ANLAGE 2
SERVICEBESCHREIBUNGEN**

Anhang 1	Symantec Email AntiVirus.cloud
Anhang 2	Symantec Email AntiSpam.Cloud
Anhang 3	Symantec Volume Mail
Anhang 4	Symantec Email Image Control.cloud
Anhang 5	Symantec Email Data Protection.cloud
Anhang 6	Symantec Email Boundary Encryption.cloud
Anhang 7	Symantec Policy Based Encryption.cloud
Anhang 8	Symantec Enterprise Instant Messenger.cloud
Anhang 9	Symantec Instant Messaging Security.cloud
Anhang 10	Symantec Web v2 Protect.cloud
Anhang 11	Symantec Web v2 URL.cloud
Anhang 12	Symantec Web v2 Smart Connect.cloud
Anhang 13	Symantec Enterprise Vault.cloud
Anhang 14	AdvisorMail on Symantec.cloud
Anhang 15	Symantec Email Continuity Archive.cloud und Symantec Email Continuity Archive Lite.cloud
Anhang 16	Symantec Email Continuity.cloud
Anhang 17	Symantec Email Archiving.cloud P
Anhang 18	Symantec Web Security Archiving.cloud
Anhang 19	Symantec Endpoint Protection Small Business Edition 2013
Anhang 20	Symantec Backup Exec.cloud

Anhang 1 – Symantec Email AntiVirus.cloud

A. Serviceübersicht

A.1. Der Symantec Email AntiVirus.cloud ("Email AV") Service scannt eingehende und ausgehende E-Mails sowie Anhänge auf Viren und Phishing-E-Mails.

B. Servicemerkmale

B.1. E-Mails werden mithilfe mehrerer Antivirus-Technologien gescannt.

B.2. Für eingehende E-Mails kann der Kunde Alarmmeldungen einrichten, die automatisch an den vorgesehenen Empfänger innerhalb des Unternehmens des Kunden sowie an einen Administrator gesendet werden, wenn der Service eine E-Mail abfängt.

B.3. Für ausgehende E-Mails kann der Kunde Alarmmeldungen einrichten, die automatisch an einen Administrator gesendet werden, wenn der Service eine E-Mail abfängt.

B.4. Bestimmte E-Mails können über die SMC automatisch freigegeben werden. Ein Administrator kann die E-Mail mit einer eindeutigen Kennung versehen und die E-Mail freigeben. Bestimmte E-Mails können nicht automatisch über die SMC freigegeben werden, wenn Symantec feststellt, dass die E-Mail wegen Virenbefalls besonders ansteckend ist oder Schäden verursacht. Der Kunde kann anfordern, dass eine nicht freigabefähige E-Mail an den vorgesehenen Empfänger oder an eine andere E-Mail-Adresse freigegeben wird, indem er sich an den technischen Support wendet und ein Freigabeformular einsendet. Einzelne Benutzer haben keinen Zugriff auf diese Quarantäne.

B.5. In Frage kommende E-Mails, die vom Service abgefangen werden, sind mindestens sieben (7) Kalendertage für die Freigabe verfügbar. Die Freigabe kann über die SMC beantragt werden.

B.6. Vom Service abgefangene E-Mails werden nicht an den Absender zurückgesendet.

B.7. Vom Service abgefangene E-Mails werden nicht an Dritte weitergeleitet.

C. Pflichten des Kunden

C.1. Der Kunde muss Konfigurationseinstellungen über die SMC festlegen, andernfalls werden die für den Service geltenden Standardeinstellungen verwendet.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen.

SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE EINE E-MAIL NICHT ABFÄNGT ODER EINE E-MAIL FÄLSCHLICHERWEISE ABFÄNGT.

Anhang 2 – Symantec Email AntiSpam.cloud

A. Serviceübersicht

A.1. Der Symantec Email AntiSpam.cloud ("Email AS") Service ist ein Scanservice für eingehende E-Mails, der dazu bestimmt ist, unerwünschte Spam-E-Mails, die eingehend an die E-Mail-Domäne des Kunden gerichtet sind, zu erkennen und das Spam-Aufkommen im Unternehmen des Kunden zu reduzieren. Der Service kann nur von Kunden abonniert werden, die auch den Email AntiVirus.cloud Service nutzen.

B. Servicebeschreibung

B.1. Beim Kunden eingehende E-Mails werden unter Verwendung verschiedener Erkennungsmethoden gescannt. Die meisten Erkennungsmethoden können vom Kunden in der SMC aktiviert oder deaktiviert werden. Bestimmte Erkennungsmethoden innerhalb des Verbindungsmanagers (Connection Manager) sind jedoch nicht konfigurierbar.

B.2. Der Kunde kann private Listen mit zugelassenen und/oder blockierten Absendern erstellen. Diese Listen werden auf eingehende E-Mails angewendet.

B.3. Maßnahmen werden für alle eingehenden E-Mails ergriffen, die vom Service als Spam identifiziert werden. Welche E-Mails als Spam identifiziert werden, hängt von den Optionen ab, die für jede Erkennungsmethode in der SMC festgelegt wurden.

B.4. Der Kunde kann in der SMC die Sender Policy Framework ("SPF")-Prüfung eingehender E-Mails aktivieren. Wenn die Domäne des Absenders eine "hard FAIL" SPF-Richtlinie veröffentlicht und die E-Mail die Authentifizierungsprüfung nicht besteht, wird die E-Mail blockiert und gelöscht. Diese blockierten und gelöschten E-Mails werden nicht in der Symantec Email Security Services-Infrastruktur empfangen und können daher nicht abgerufen oder isoliert werden. Wenn die versendende Domäne eine andere SPF-Richtlinie als "hard FAIL" oder keine SPF-Richtlinie veröffentlicht, ist das SPF-Prüfergebnis neutral und die E-Mail wird nicht blockiert oder gelöscht.

B.5. Für alle anderen eingehenden Email AntiSpam.cloud-Erkennungsmethoden können die folgenden Optionen vom Kunden ausgewählt werden, um festzulegen, welche Maßnahmen für eingehende E-Mails ergriffen werden sollen, die vom Service als Spam identifiziert werden:

- a) Markieren verdächtiger E-Mails im Header
- b) Markieren verdächtiger E-Mails in der Betreffzeile (der Kunde kann den Text angeben, der in Betreffzeilen hinzugefügt werden soll)
- c) Umleiten verdächtiger E-Mails an eine vorher definierte E-Mail-Adresse (die sich in einer vom Service gescannten Domäne befinden muss)
- d) Blockieren und Löschen verdächtiger E-Mails
- e) Isolieren der E-Mail (falls diese Option aktiviert ist)

B.6. Falls der Kunde die Option "End User Email Quarantine" für den Service aktiviert hat, kann der Kunde die Isolierung von E-Mails als Maßnahme für alle eingehenden E-Mails auswählen, die vom Service als Spam identifiziert werden. In der Quarantäne sind folgende Optionen verfügbar:

- a) Löschen der E-Mail
- b) Zustellen der E-Mail an die ursprüngliche Empfängeradresse
- c) Überprüfen des Texts der E-Mail

B.7. Der Kunde kann für den Zweck eines E-Mail-Aliasing und delegierten Zugangs eine Reihe einzelner E-Mail-Adressen mit einer "Inhaber"-E-Mail-Adresse verknüpfen. Maximal dürfen hierbei fünfzig (50) E-Mail-Adressen mit einer einzelnen E-Mail-Adresse verknüpft werden. Symantec behält sich das Recht vor, die Kontogruppe bzw. die Aliasing-Verknüpfungen des Kunden zu entfernen, wenn diese Höchstzahl überschritten wird.

C. Pflichten des Kunden

C.1. Der Kunde kann Einstellungsoptionen für eingehende E-Mails über die SMC anpassen. Falls keine Anpassung erfolgt, werden die Standardeinstellungen des Service für jede der vom Kunden ausgewählten Domänen übernommen.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE SPAM NICHT ERKENNT ODER LEGITIME E-MAIL FÄLSCHLICHERWEISE ALS SPAM IDENTIFIZIERT.

Anhang 3 – Symantec Volume Mail

A. Serviceübersicht

A.1. Der Symantec Volume Mail ("Email VM") Service ermöglicht es dem Kunden, Massen-E-Mail (Volume Mail) zu senden und zu empfangen. Ein Kunde, der regelmäßig E-Mails an mehr als 500 Empfänger sendet oder regelmäßig Antwort-E-Mails von 500 oder mehr E-Mail-Adressen empfängt, wobei die Gesamtzahl innerhalb von dreißig (30) Kalendertagen 5.000 E-Mails überschreitet, ist verpflichtet, den Volume Mail Service zu abonnieren. Der Service kann nur von Kunden abonniert werden, die auch den Email AntiVirus.cloud Service nutzen.

B. Servicemerkmale

B.1. Die Massen-E-Mail darf nur an Empfänger gerichtet sein, die einem Empfang solcher E-Mails ausdrücklich zugestimmt haben (Opt-in-Empfänger).

B.2. Massen-E-Mails einschließlich der Anhänge dürfen eine Größe von 500 KB nicht überschreiten.

B.3. Das Empfänger-Adressfeld in jeder Massen-E-Mail darf pro E-Mail nicht mehr als fünfhundert (500) E-Mail-Adressen enthalten.

B.4. Der Kunde hat die Menge der zu versendenden bzw. empfangenden Massen-E-Mails auf maximal 250.000 Empfänger pro Kalendertag zu begrenzen.

B.5. Für jede Preiskategorie des Volume Mail Service gilt eine maximale Quote zulässiger Empfänger pro Monat. Diese Quoten sind nicht übertragbar oder addierbar; aus diesem Grund ist keine Übertragung ungenutzter Empfängerquoten auf nachfolgende Monate möglich.

C. Pflichten des Kunden.

C.1. Der Kunde muss ein effektives Listenverwaltungssystem führen, mit dem unter anderem E-Mail-Adressen unverzüglich entfernt werden können, die ungültig bzw. infolge einer Kündigung zu löschen sind.

C.2. Der Kunde muss sicherstellen, dass der Haftungsausschlusstext für ausgehende Nachrichten den Empfänger darüber benachrichtigt, dass die Massen-E-Mails auf Viren überprüft wurden.

C.3. Der Kunde hat Symantec zu benachrichtigen, wenn bei der tatsächlichen Nutzung des Volume Mail Service zu irgendeinem Zeitpunkt die Anzahl der pro Monat zulässigen Empfänger für die vom Kunden genutzte Preiskategorie überschritten wird. Dies hat zur Folge, dass Symantec die Gebühr für die jeweilige Preiskategorie gemäß der dann aktuellen Preisliste von Symantec erhöhen wird. Symantec wird die Nutzung überwachen und den Kunden bei einer Überschreitung der maximal zulässigen Menge benachrichtigen.

C.4. Symantec empfiehlt dem Kunden, eine separate Domäne für das Versenden von Massen-E-Mails zu verwenden.

C.5. Symantec empfiehlt, dass der Kunde das Versenden von Massen-E-Mails staffelt und Massen-E-Mails außerhalb der örtlichen Geschäftszeiten versendet.

C.6. Der Kunde ist verpflichtet, auf Verlangen von Symantec sowie vorbehaltlich der geltenden Gesetze nachzuweisen, dass die Massen-E-Mails nur an Empfänger gerichtet sind, die einem Empfang solcher E-Mails ausdrücklich zugestimmt haben (Opt-in-Empfänger), und dass die E-Mail kein Spam enthält.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. DER KUNDE ERKLÄRT SICH DAMIT EINVERSTANDEN, DASS SYMANTEC VOM KUNDEN VERLANGEN KANN, AUF DEN VOLUME MAIL SERVICE ZU MIGRIEREN, FALLS SICH DAS E-MAIL-DATENVERKEHRSPROFIL NACHTEILIG AUF ANDERE KUNDEN AUSWIRKT.

F.2. Der Kunde erkennt an und akzeptiert, dass das Versenden von Massen-E-Mails mit Wahrscheinlichkeit wechselnde Auswirkungen auf den E-Mail-Datenverkehr haben kann. Derartige Auswirkungen entziehen sich der Kontrolle durch Symantec; aus diesem Grund gelten die im Service Level Agreement aufgeführten Service Level für die Serviceverfügbarkeit und Latenz nicht für den Volume Mail Service. Die SLAs für Email AntiVirus.cloud und Email AntiSpam.cloud sind jedoch weiterhin gültig.

F.3. Falls zu irgendeinem Zeitpunkt (i) die E-Mail-Systeme des Kunden auf eine Sperrliste gesetzt werden, (ii) der Kunde verursacht, dass die Symantec-Systeme auf eine Sperrliste gesetzt werden, weil Spam versendet wurde, oder (iii) der Kunde den in diesem Anhang dargelegten Verpflichtungen nicht nachkommt, ist Symantec verpflichtet, den Kunden darüber zu informieren; in diesem Fall behält sich Symantec das Recht vor, im eigenen

Ermessen umgehend die Bereitstellung des Service ganz oder teilweise zu verweigern bzw. vorübergehend auszusetzen oder komplett einzustellen.

F.4. Der Volume Mail Service wird nach der Anzahl der Empfänger bemessen. Ein Kunde, der eine E-Mail an 1.000 Empfänger sendet, ist einem Kunden gleichgestellt, der dieselbe E-Mail 1.000-Mal versendet – beides gilt gemäß diesem Service als Massen-E-Mail.

F.5. Massen-E-Mails können ein- und ausgehende E-Mails sein.

F.6. Falls die Nutzung des Volume Mail Service durch den Kunden dessen vereinbarte Preiskategorie überschreitet, wird eine Zusatzgebühr für die übermäßige Nutzung pro 1.000 zusätzlicher E-Mail-Empfänger erhoben.

F.7. Die oberste Preiskategorie deckt maximal 1.000.000 Empfänger pro Monat ab. Für den Fall, dass der Bedarf des Kunden über diese maximale Nutzung hinausgeht, muss Symantec prüfen, ob eine solche Nutzung betrieblich durchführbar ist.

F.8. Der Volume Mail Service wird vierteljährlich in Rechnung gestellt.

F.9. Für den Volume Mail Service gilt keine Mindestlaufzeit. Jede der beiden Parteien kann den Service mit einer Kündigungsfrist von drei (3) Monaten kündigen.

Anhang 4 – Symantec Email Image Control.cloud

A. Serviceübersicht

A.1. Der Symantec Email Image Control.cloud ("Email IC") Service ist ein Scanservice, der die eingehenden und ausgehenden E-Mails des Kunden scannt, um pornographische Bilder zu erkennen. Der Service kann nur von Kunden abonniert werden, die auch den Email AntiVirus.cloud Service nutzen.

B. Servicemerkmale

B.1. Der Service wird für alle vom Kunden festgelegte Domänen aktiviert.

B.2. E-Mails werden mithilfe von Image Composition Analysis-Technologie auf pornographische Bilder gescannt.

B.3. Der Service kann nur bestimmte Dateitypen auf pornographische Bilder scannen. Diese Dateitypen sind im Administratorhandbuch und in der Online-Hilfe für den Service definiert.

B.4. Maßnahmen und Benachrichtigungen werden pro E-Mail, in der der Service ein pornographisches Bild erkennt, ergriffen. Diese hängen von den Optionen ab, die der Kunde in der SMC einstellt.

B.5. Die folgenden Optionen stehen dem Kunden zur Festlegung von zu ergreifenden Maßnahmen zur Verfügung, falls der Service ein pornographisches Bild in einer E-Mail erkennt. Diese Optionen können für ein- und ausgehende E-Mails unabhängig voneinander festgelegt werden:

- a) Protokollieren verdächtiger E-Mails (liefert Statistiken, die über die SMC eingesehen werden können)
- b) Markieren verdächtiger E-Mails im Header (gilt nur für eingehende E-Mails)
- c) Markieren verdächtiger E-Mails in der Betreffzeile (gilt nur für eingehende E-Mails)
- d) Senden einer Kopie verdächtiger E-Mails an eine vorgegebene E-Mail-Adresse
- e) Umleiten verdächtiger E-Mails an eine vorgegebene E-Mail-Adresse
- f) Blockieren und Löschen verdächtiger E-Mails

B.6. Der Kunde kann für die Verwaltung des Service zugelassene E-Mail-Absender oder -Empfänger in der SMC identifizieren. Die E-Mails dieser Absender und Empfänger werden dann nicht vom Service gescannt.

B.7. Der Kunde kann über die SMC spezielle zugelassene oder blockierte Bilder festlegen. Zugelassene Bilder werden vom Service nicht blockiert.

C. Pflichten des Kunden

C.1. Der Kunde muss die Konfigurationsoptionen für jede Domäne, für die er den Service bezieht, über die SMC festlegen, andernfalls werden die für den Service geltenden Standardeinstellungen verwendet.

D. **Berichterstattung.** Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. **Technischer Support.** Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Der Kunde erkennt an, dass die Identifizierung eines pornographischen Bilds subjektiv ist und auf der automatisierten Scantechnologie basiert.

F.2. Der Service kann ggf. keine Anhänge mit Inhalt scannen, der direkt vom Absender kontrolliert wird (z. B. kennwortgeschützte und/oder verschlüsselte Anhänge).

F.3. Unter keinen Umständen dürfen illegale Bilder an Symantec gesendet werden. Der Kunde sollte sich an die örtliche Polizeibehörde wenden, um sich zu erkundigen, wie er mit solchen Bildern verfahren soll.

F.4. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE EIN PORNOGRAPHISCHES BILD NICHT ERKENNT ODER EIN BILD FÄLSCHLICHERWEISE ALS PORNOGRAPHIEVERDÄCHTIG IDENTIFIZIERT.

Anhang 5 – Symantec Email Data Protection.cloud

A. Serviceübersicht

A.1. Der Symantec Email Data Protection.cloud ("Email DP") Service ist ein Scanservice, mit dem der Kunde eine eigene regelgesteuerte Filterstrategie für E-Mails konfigurieren kann. Der Service kann nur von Kunden abonniert werden, die auch den Email AntiVirus.cloud Service nutzen.

B. Servicemerkmale

B.1. Der Kunde kann eine Reihe von Richtlinien erstellen, nach dem ein- und ausgehende E-Mails vom Service gefiltert werden.

B.2. Eine Richtlinie ist eine vom Kunden erstellte Gruppe von Regeln oder Anweisungen, mit deren Hilfe bestimmte Formate von Nachrichten/Anhängen sowie Inhalte innerhalb einer E-Mail identifiziert werden. Die Richtlinie legt fest, welche Maßnahme zu ergreifen ist, wenn das angegebene Format in einer E-Mail vorkommt.

B.3. Der Kunde kann Richtlinien "global", "pro Domäne" oder "pro Gruppe" konfigurieren.

B.4. Der Service funktioniert auf der Grundlage eines exakten Abgleichs mit den vom Kunden konfigurierten Richtlinien. Der Service gleicht so lange alle Richtlinien ab, bis er ein Exit-Ereignis ermittelt und den Scanvorgang abschließt.

B.5. Der Service kann nur bestimmte Dateitypen auf Inhalte scannen. Diese Dateitypen sind im Administratorhandbuch und in der Online-Hilfe für den Service definiert.

B.6. Die folgenden Optionen stehen dem Kunden zur Festlegung von zu ergreifenden Maßnahmen zur Verfügung, falls der Service für eine E-Mail eine Übereinstimmung mit einer vom Kunden definierten Richtlinie erkennt. Sämtliche Maßnahmen können nach Bedarf als Exit-Ereignis aktiviert werden.

Diese Optionen können für ein- und ausgehende E-Mails unabhängig voneinander festgelegt werden:

- a) Blockieren und Löschen verdächtiger E-Mails (Standard-Exit-Ereignis)
- b) Markieren (gilt nur für eingehende E-Mails) und Umleiten verdächtiger E-Mails an einen angegebenen Administrator (Standard-Exit-Ereignis)
- c) Markieren (gilt nur für eingehende E-Mails) und Versenden einer Kopie verdächtiger E-Mails an einen angegebenen Administrator
- d) Markieren (gilt nur für eingehende E-Mails) des Headers verdächtiger E-Mails
- e) Komprimieren von E-Mail-Anhängen
- f) Nur Protokollieren für SMC-Statistiken
- g) Markieren in der Betreffzeile
- h) Weiterleiten an eine bestimmte IP-Adresse oder einen bestimmten Hostnamen
- i) Zulassen (Standard-Exit-Ereignis)

B.7. Der Kunde kann über die SMC Benachrichtigungen, die er für einzelne Richtlinien konfiguriert hat, aktivieren, deaktivieren und ändern.

B.8. Vorlagen, Wörterbücher, Listen und reguläre Ausdrücke werden mit dem Service bereitgestellt. Der Kunden kann diese Vorlagen nutzen, um eigene Richtlinien zu definieren oder eigene angepasste Listen und reguläre Ausdrücke zu erstellen.

B.9. Symantec ist nicht dafür verantwortlich, Support oder Fehlerbehebung für vom Kunden definierte reguläre Ausdrücke bereitzustellen.

B.10. Auf Anfrage vom Kunden wird Symantec wirtschaftlich angemessene Anstrengungen unternehmen, um angepasste reguläre Ausdrücke zu erstellen, um das gewünschte Ergebnis zu erzielen.

C. Pflichten des Kunden

C.1. Der Kunde ist selbst für die Implementierung der Konfigurationsoptionen für den Service für jede Domäne verantwortlich. Die Konfiguration ist über die SMC vorzunehmen.

C.2. Der Kunde muss die Richtlinien in einer logischen Hierarchie implementieren, da andernfalls eine Richtlinie ggf. nicht angewendet wird, bevor der Service das vom Kunden festgelegte Exit-Ereignis erreicht.

C.3. Der Kunde ist dafür verantwortlich, von Symantec bereitgestellte reguläre Ausdrücke zu testen, um festzustellen, ob das gewünschte Ergebnis erzielt werden kann.

D. Berichterstattung.

D.1. Der Kunde kann sich für die Aktivierung einer optionalen Funktion entscheiden, um Berichte basierend auf abgeglichenen Inhalt und einem Teil des umgebenden Texts zu erstellen. Falls der Kunde diese Funktion aktiviert, wird der abgeglichene Inhalt standardmäßig redigiert und nicht protokolliert. Der Kunde kann die Redaktionsfunktion deaktivieren. Danach wird der abgeglichene Inhalt ggf. protokolliert und in die Berichtsdaten aufgenommen. Der Kunde versteht, dass die Redaktion eine optionale Funktion ist, die nur auf abgeglichenen

Inhalt angewendet wird, und der Service keinen Text redigiert, der den abgeglichenen Inhalt umgibt. Es unterliegt der alleinigen Verantwortung des Kunden, die Datenerfassung und Erstellung entsprechender Berichte über diese Funktion zu verwalten.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Der Kunde akzeptiert, dass, falls der Service zusammen mit der Quarantänefunktion des Email AntiSpam.cloud Service genutzt wird, dies dazu führen kann, dass eine E-Mail isoliert werden kann, bevor sie vom Service gefiltert wurde.

F.2. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE EINE E-MAIL MIT VERDÄCHTIGEM INHALT NICHT ERKENNT ODER EINE E-MAIL FÄLSCHLICHERWEISE ALS EINE E-MAIL MIT VERDÄCHTIGEM INHALT IDENTIFIZIERT.

Anhang 6 – Symantec Email Boundary Encryption.cloud

A. Serviceübersicht

A.1. Der Symantec Email Boundary Encryption.cloud ("Email BE") Service bietet verschlüsselte Kommunikationskanäle für die Kommunikation des Kunden mit ausgewählten Drittparteien. Der Service kann nur von Kunden abonniert werden, die auch den Email AntiVirus.cloud Service nutzen.

B. Servicemerkmale

B.1. Der Service basiert auf dem Standard "SMTP over TLS" (Simple Mail Transfer Protocol over Transport Layer Security).

B.2. Der Kunde kann ein sicheres privates E-Mail-Netzwerk (Secure Private Email Network, SPEN) mit ausgewählten Drittparteien ("SPEN-Partner") aufbauen. Diese Konfiguration wird als "Enforced"-Verschlüsselung bezeichnet.

B.3. Der Kunde kann seine E-Mail-Server auch für das Servicemodell "Secure Connect" (Sichere Verbindung) konfigurieren. In diesem Fall gilt:

- a) Der Austausch von E-Mails zwischen Symantec und den mit "Secure Connect" betriebenen Mail-Servern des Kunden wird durch TLS-Verschlüsselung gesichert. Ob das weitergehende Routing in nicht-verschlüsseltem oder verschlüsseltem Format durchgeführt wird, hängt ab (i) von den durch den Kunden festgelegten TLS-Erzwingungen und (ii) von der Fähigkeit des Zielservers zum Empfang von E-Mails über Opportunistic TLS.

B.4. Falls der Kunde den Service in Verbindung mit dem Policy Based Encryption.cloud Service verwendet, muss er das "Secure Connect"-Modell des Service auf allen seinen Mail-Servern implementieren.

B.5. Zertifikate und Authentifizierung:

- a) Wenn der Kunde eine TLS-Verbindung herstellt, muss der akzeptierende Mail-Server zur Authentifizierung sein Zertifikat vorlegen. Wenn der akzeptierende Mail-Server die Authentifizierung des Service wünscht, so wird Symantec sein Clientzertifikat zur Authentifizierung vorlegen. Wenn der akzeptierende Mail-Server die E-Mail nicht authentifizieren kann, wird die E-Mail an den Kunden zurückgesendet.
- b) Wenn ein externer Mail-Server eine TLS-Verbindung herstellt, wird der Service sein Serverzertifikat zur Authentifizierung vorlegen, jedoch nicht anfordern, dass der externe Mail-Server sein Clientzertifikat zur Authentifizierung vorlegt.
- c) Die Validierung eines Zertifikats obliegt der Zertifizierungsstelle (Certificate Authority), die das Zertifikat signiert hat. Für jedes von einem externen Mail-Server als Teil einer TLS-Verbindung unterbreitete Zertifikat wird der Service bestätigen, dass eine anerkannte Zertifizierungsstelle das Zertifikat signiert hat. Wenn ein Zertifikat nicht von einer anerkannten Zertifizierungsstelle validiert werden kann, wird die Verbindung abgebrochen und die E-Mail an den Absender zurückgesendet. Eine Liste der anerkannten Zertifizierungsstellen ist auf Anfrage erhältlich.

C. Pflichten des Kunden

C.1. Der Kunde muss SPEN-Partner für jede Domäne definieren. Die SPEN-Partner müssen keine Kunden des Email Boundary Encryption.cloud Service sein, jedoch unterstützt Symantec keine SPEN-Partner direkt, die nicht Kunden des Email Boundary Encryption.cloud Service sind.

C.2. Damit der Service genutzt werden kann, müssen sowohl der Mail-Server des Kunden als auch der Mail-Server des SPEN-Partners TLS unterstützen.

C.3. Wenn ein Kunde auch den Email AntiSpam.cloud Service nutzt, muss er die Domänen seiner SPEN-Partner in eine Liste mit genehmigten E-Mail-Absendern aufnehmen. Andernfalls kann unter bestimmten Umständen, bei denen die Nichtverfügbarkeit des lokalen Signatursystems auftritt, die E-Mail über ein öffentliches Netzwerk zu einem Remote-Signatursystem umgeleitet wird.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support.

E.1. Die in Anlage 1 definierten Reaktionszeiten des Kundensupports gelten nicht für die Bereitstellung dieses Service.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Symantec übernimmt keine Haftung, wenn der Kunde oder ein Dritter (einschließlich, aber nicht darauf beschränkt, SPEN-Partner) seine Pflichten bezüglich der Registrierung von Zertifikaten nicht erfüllt. Ferner haftet Symantec nicht für das rechtzeitige Vorliegen oder die Richtigkeit dieser Informationen.

F.2. DER KUNDE AKZEPTIERT, DASS BEI ANWENDUNG DES MODELLS "SECURE CONNECT" NUR SERVER, DIE IN "OUTBOUND ROUTES" REGISTRIERT SIND, ÜBER TLS VERSCHLÜSSELT WERDEN. AUF SERVERN, DIE NICHT IN DIESEM ABSCHNITT KONFIGURIERT SIND, WIRD DIE TLS-VERSCHLÜSSELUNG GGF. NICHT ERZWUNGEN.

Anhang 7 – Symantec Policy Based Encryption.cloud

A. Serviceübersicht

A.1. Der Symantec Policy Based Encryption.cloud ("Email PBE") Service ermöglicht das Senden und Empfangen verschlüsselter E-Mails. Um Email PBE beziehen zu können, muss der Kunde auch folgende Services abonnieren: Email Boundary Encryption.cloud Service und Email Data Protection.cloud Service. Jeder Policy Based Encryption.cloud-Benutzer muss auch ein Email Data Protection.cloud-Benutzer sein.

B. Servicemerkmale

B.1. Der Kunde muss Email Data Protection.cloud zum Definieren von Richtlinien für die Verschlüsselung ausgehender E-Mails nutzen.

B.2. Der Kunde kann als Verschlüsselungsmethode entweder Push oder Pull konfigurieren. Für Symantec Policy Based Encryption.cloud (Z) ("PBE Z") wird durch die Email Data Protection.cloud-Richtlinie festgelegt, ob Push oder Pull konfiguriert wird. Für Symantec Policy Based Encryption.cloud (E) ("PBE E") ist die standardmäßige Verschlüsselungsmethode Pull, die jedoch durch den Empfänger in Push geändert werden kann, wenn diese Konfiguration vom Absender ausgewählt wird.

- a) Bei der Variante "PBE Push" des Policy Based Encryption.cloud Service wird eine E-Mail-Benachrichtigung an den Empfänger gesendet, in der die ursprüngliche E-Mail als verschlüsselter Anhang gespeichert ist. Nach der anfänglichen Online-Registrierung für den Policy Based Encryption.cloud (E) Service kann der Empfänger die entschlüsselte E-Mail offline mithilfe eines sicheren Readers ansehen.
- b) Bei der Variante "PBE Pull" des Service wird eine E-Mail-Benachrichtigung an den Empfänger gesendet. Der Empfänger kann die entschlüsselte E-Mail online über eine sichere SSL-Sitzung in seinem Browser ansehen, wenn er sich bei einem sicheren Web-Portal einloggt und sein Kennwort eingibt.

B.3. Der Kunde kann einen Teil des Portals, über das die Empfänger die verschlüsselten E-Mails lesen, anpassen. Falls keine Anpassung erfolgt, werden die Standardeinstellungen des Service übernommen.

B.4. Der Empfänger einer verschlüsselten E-Mail kann auch eine verschlüsselte E-Mail an Email PBE-Benutzer des Kunden senden.

B.5. Wenn der Kunde den Service abonniert, steht ein Drittanbieter-Plugin für Microsoft Outlook® zur Verfügung, das der Microsoft Outlook®-Werkzeugleiste des Empfängers ein "Verschlüsseln"-Symbol hinzufügt. Der Kunde kann dieses Plugin nach eigenem Ermessen verwenden. Dieses Plugin wird von Symantec weder direkt unterstützt noch übernimmt Symantec irgendeine Verantwortung für das Plugin.

B.6. Für Email PBE gelten folgende Einschränkungen:

- a) Die Anzahl der sicheren E-Mails, die Kunden monatlich über Policy Based Encryption.cloud (Z) versenden dürfen, darf nicht dreihundert (300) Mal die Anzahl der Benutzer des Service überschreiten.
- b) Die Anzahl der sicheren E-Mails, die Kunden monatlich über Policy Based Encryption.cloud (Z) versenden dürfen, darf nicht vierhundertachtzig (480) Mal die Anzahl der Benutzer des Service überschreiten.
- c) Beim Versenden an mehrere Empfänger wird jede eindeutige Adresse als eine sichere E-Mail gezählt. Falls der Kunde die Zahl der zulässigen sicheren E-Mails pro Monat überschreitet, behält sich Symantec das Recht vor, dem Kunden dies entsprechend in Rechnung zu stellen.
- d) Über den Policy Based Encryption.cloud (Z) Service geleitete E-Mails sind komprimiert auf eine maximale Größe von fünfzig Megabyte (50 MB) pro E-Mail beschränkt. Über den Policy Based Encryption.cloud (E) Service geleitete E-Mails sind auf eine maximale Größe von fünfzig Megabyte (50 MB) pro E-Mail-Nachverschlüsselung beschränkt.

C. Pflichten des Kunden

C.1. Der Kunde ist selbst für die Implementierung der Konfigurationsoptionen für den Service verantwortlich. Die Konfiguration ist über die SMC vorzunehmen.

C.2. Der Kunde kann maximal zwei Mal in einem Zeitraum von 12 Monaten eine Anpassung von Teilen des Portals, für die eine Anpassung möglich ist und die von Empfängern zum Lesen verschlüsselter E-Mails genutzt werden, anfordern.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support.

E.1. Die in Anlage 1 definierten Reaktionszeiten des Kundensupports gelten nicht für die Bereitstellung dieses Service.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Der im Service Level Agreement festgelegte Service Level für die E-Mail-Latenz gilt nicht für diesen Service.

F.2. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE E-MAILS NICHT VERSCHLÜSSELT.

Anhang 8 – Symantec Enterprise Instant Messenger.cloud

A. Serviceübersicht

A.1. Der Symantec Enterprise Instant Messenger.cloud ("EIM") Service ermöglicht die administrative Kontrolle, zentralisierte Speicherung und Domänenverwaltung von Instant Messages.

B. Servicemerkmale

B.1. Jede der nachfolgend beschriebenen Versionen des Service ermöglicht Benutzern, eine sichere Verbindung zur Serviceplattform herzustellen und den Service zu nutzen.

B.2. Mit Ausnahme der MSI- und Java-Versionen wird der Serviceclient ("POD" oder "Servicesoftware") auf der Arbeitsstation jedes Benutzers installiert. Der POD hat die folgenden Funktionen:

- a) Austauschen von Dateien (File Sharing)
- b) Sichere Konferenzen über Instant Messaging
- c) Interoperabilität mit öffentlichen Instant Messaging-Netzwerken (nur mit dem CONNECT-Paket)

B.3. Die SMC ermöglicht es ausgewiesenen Administratoren, ihre Domänenstruktur und Benutzerbasis zu verwalten.

B.4. Symantec Enterprise Instant Message.cloud Communicate.cloud ("COMMUNICATE") Option

- a) Integriertes File Sharing (100 MB Kapazität pro Benutzer)
- b) Backup-Lösung auf dem Desktop
- c) Möglichkeit, Informationen mit Instant Messaging Security.cloud-Benutzern gemeinsam zu nutzen, die online oder offline sind
- d) Zugangskontrolllisten
- e) Sichere, 168-Bit 3DES SSL verschlüsselte POD-to-POD Kommunikation
- f) Webbasierte Verwaltungskonsole
- g) Umfassende Optionen für die Benutzeroberfläche
- h) Erweiterte Echtzeiterkennung und -verfolgung
- i) Unterstützung einer großen Auswahl von Proxy-Servern
- j) HTTP-Tunneling-Fähigkeiten
- k) Alarmmeldungen bei neuen Dateien
- l) Objektorientiertes Dateisystem mit umfangreichen Suchfunktionen

B.5. Symantec Enterprise Instant Message.cloud Connect.cloud ("CONNECT") Option

Alle Funktionen des COMMUNICATE-Pakets plus:

- a) Interoperable Instant Messenger (AOL®, MSN®, Yahoo! ®)
- b) SMS-Nachrichten (2 Nachrichten pro Benutzer oder "Benutzerquoten")
- c) Protokollfunktionen für Instant Messaging

B.6. Der Kunde hat die Möglichkeit, Instant Messages, die über den Service weitergeleitet werden, zu protokollieren.

B.7. Symantec bewahrt Protokolle für einen Zeitraum von drei (3) Jahren auf. Nach Ablauf dieser Frist werden die Protokolle dauerhaft gelöscht. Der Kunde kann jederzeit vor Ablauf der vorgenannten dreijährigen (3) Aufbewahrungsfrist auf schriftliche Anfrage (i) eine Kopie dieser Protokolle anfordern oder verlangen, (ii) dass die Protokolle gelöscht werden.

C. Pflichten des Kunden

C.1. Der Kunde ist für alle vom Kunden autorisierten oder nicht autorisierten Nutzungen der Administrations-Website ebenso verantwortlich wie für die Geheimhaltung der Logins und Kennwörter für das Konto des Kunden. Der Kunde verpflichtet sich, Symantec jede nicht autorisierte Nutzung des Kundenkontos unverzüglich anzuzeigen.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. Der Kunde stimmt zu, dass Symantec eine zusätzliche Gebühr für Instant Messaging-Protokolle berechnen kann, die älter als ein (1) Jahr sind.

F.2. Der Kunde erkennt an, dass er die Protokollierung über die SMC jederzeit für bestimmte Gruppen oder Teilgruppen deaktivieren kann und die Protokolle deshalb möglicherweise keinen vollständigen Datensatz der Nutzung des Service durch den Kunden liefern.

F.3. Nach Kündigung des Service kann der Kunde die Aushändigung oder Löschung seiner Protokolle anfordern. Wenn der Kunde es versäumt, innerhalb von neunzig (90) Kalendertagen nach Inkrafttreten der Kündigung sich für eine der beiden Optionen zu entscheiden, werden die Protokolle dauerhaft gelöscht.

F.4. Symantec kann unter keinen Umständen die Funktion eines Drittanbieter-Downloaders im Sinne der SEC-Bestimmungen übernehmen.

F.5. Dem Kunden wird die Interoperabilitätsfunktion wie in diesem Anhang beschrieben (siehe CONNECT-Paket oben) zur Verfügung gestellt. Symantec übernimmt keine Gewähr bzw. bietet keine Garantie bezüglich der Fähigkeit des Services hinsichtlich der Interoperabilität mit anderen Instant Messaging-Anbietern wie insbesondere AOL®, MSN® und Yahoo!®.

F.6. **Nutzungsrichtlinie.** Der Kunde verpflichtet sich:

- a) Keine Daten, Texte, Videos, Audios, Software oder andere Inhalte, die illegal sind, über den POD oder den Service zu übertragen oder zu speichern.
- b) Keine Inhalte, die Patente, Marken, Urheberrechte, Veröffentlichungsrechte oder sonstige geistige Eigentumsrechte verletzen, über den POD oder den Service zu übertragen oder zu speichern.
- c) Keine Inhalte, die gegen regionale, staatliche, nationale oder internationale Gesetze verstoßen und die eine zivil- oder strafrechtliche Haftung begründen könnten, zu übertragen oder zu speichern.
- d) Keine unerwünschten verkaufsfördernden Inhalte, Werbematerialien, Spam, "Spim" (über Instant Messaging übertragene Spam-Nachrichten), Kettenbriefe oder sonstige Werbung zu übertragen.
- e) Den POD oder den Service nicht zur öffentlichen Übertragung, Übermittlung oder Vorführung außer zu Unternehmenszwecken zu nutzen.
- f) Den POD oder den Service nicht für die absichtliche Übertragung von Inhalten zu nutzen, die Viren, Würmer, Cancelbots, Zeitbomben, Trojaner, Sniffer oder sonstigen Code enthalten, der zum Erlangen von Informationen über andere Benutzer oder zur Unterbrechung der Funktionalität oder Verfügbarkeit von Computerprogrammen, Datenbanken, des Service oder sonstiger Internet-Hosts bestimmt ist.
- g) Die Identität des POD-Benutzers nicht durch Spoofing, Fälschung von Headern, die Verwendung von weiterleitenden Dritten oder anderweitig die Verschleierung der Herkunft des übertragenen Inhalts, insbesondere die Nachahmung einer anderen natürlichen oder juristischen Person, zu verbergen.

F.7. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

h)

Anhang 9 – Symantec Instant Messaging Security.cloud

A. Serviceübersicht

A.1. Der Symantec Instant Messaging Security.cloud ("IMS") Service scannt Instant Messages und Anhänge auf Malware, bösartige URL-Links und unangemessene Inhalte. Jede Nachricht kann zudem vom Kunden protokolliert werden.

B. Servicemerkmale

B.1. Sobald der Service vom Kunden konfiguriert wurde, werden Instant Messages aus unterstützten UC- und IM-Plattformen durch den Service geleitet und gescannt.

B.2. Der Service kann nur bestimmte Versionen von UC- und IM-Clients scannen. Eine Liste der neuesten unterstützten Versionen kann vom technischen Support angefordert werden. Der Kunde erkennt an und stimmt zu, dass Symantec diese Liste ohne vorherige Ankündigung aktualisieren und ändern kann.

B.3. Wenn eine Instant Messaging-Nachricht:

- a) als virenfiziert oder als mit anderem bösartigen Code infiziert eingestuft wird, wird sie blockiert
- b) eine URL für eine Website enthält, auf der ein Virus oder anderer bösartiger Code gefunden wurde, wird sie blockiert

B.4. Instant Messaging Security.cloud kann Anhänge auf bösartigen Code scannen.

B.5. Instant Messaging Security.cloud Content Control ("IMS CC")

B.5.1. Der Kunde kann eine eigene Regel basierend auf der Filterstrategie für Inhalte für eingehende und ausgehende Instant Messages konfigurieren. Die Konfiguration ist über die SMC vorzunehmen.

B.5.2. Die Regeln können auf Gruppen- oder individueller Basis konfiguriert werden.

B.5.3. Es stehen Optionen zum Definieren der Maßnahme zur Verfügung, die beim Erkennen kontrollierter Inhalte in einer Instant Message durchzuführen ist. Diese Optionen sind in der SMC und in der aktuellen Version des Administratorhandbuchs ausführlich beschrieben.

B.5.4. Der Service kann Dateinamen von Anhängen, jedoch nicht den Textteil eines Anhangs scannen.

B.6. Protokolle und Speicherung

B.6.1. Wenn der Kunde die Protokollfunktion aktiviert hat, erstellt Symantec tägliche Protokolle zu gescannten Instant Messages. In jedem Protokoll sind Datums- und Zeitstempel, Inhalte sowie die Namen der übertragenen Dateien aufzuführen. Protokolle, die dem Kunden nicht zugestellt werden können, sind einunddreißig (31) Kalendertage lang zu speichern und anschließend zu vernichten.

B.6.2. Der Kunde kann den Service über die SMC außerdem so konfigurieren, dass von jeder Instant Messaging-Nachricht eine Kopie an eine bestimmte E-Mail-Adresse gesendet wird.

B.7. Benachrichtigungen

B.7.1. Der Kunde kann den Service so konfigurieren, dass automatisch Benachrichtigungen an den Absender und den vorgesehenen Empfänger gesendet werden, falls eine Instant Message blockiert wird, wenn angenommen wird, dass sie einen Virus, einen Phishing-Angriff, eine bösartige URL oder kontrollierten Inhalt enthält.

C. Pflichten des Kunden

C.1. Der Kunde kann Einstellungsoptionen über die SMC anpassen. Falls keine Anpassung erfolgt, werden die Standardeinstellungen des Service übernommen.

C.2. Der Kunde muss sein Benutzerverzeichnis mit Symantec synchronisieren, um eine Liste mit Active Directory-Benutzernamen und zugehörigen Instant Messaging-Benutzernamen in der SMC zu erstellen. Ein "interner Benutzer" ist entweder ein unterstützter öffentlicher Instant Messaging-Benutzer oder ein unterstützter UC-Benutzer, der über eine vom Kunden bereitgestellte IP-Adresse auf Instant Messaging Security.cloud zugreift, oder ein Roaming-Benutzer, der über eine vom Kunden bereitgestellte SIP-Domäne auf Instant Messaging Security.cloud zugreift. Ein "externer Benutzer" ist jeder Benutzer, der die oben genannten Kriterien nicht erfüllt.

D. **Berichterstattung.** Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. **Technischer Support.** Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1 SYMANTEC ÜBERNIMMT KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE SPIM, VIREN, PHISHING-ANGRIFFE,

BÖSARTIGEN CODE, BLOCKIERTE URL-ADRESSEN ODER KONTROLLIERTE INHALTE NICHT ERKENNT ODER DASS DER SERVICE INSTANT MESSAGES FÄLSCHLICHERWEISE ALS INSTANT MESSAGES IDENTIFIZIERT, DIE SPIM, VIREN, PHISHING-ANGRIFFE, BÖSARTIGEN CODE, BLOCKIERTE URL-ADRESSEN ODER KONTROLLIERTE INHALTE ENTHALTEN.

F.2. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

Anhang 10 – Symantec Web v2 Protect.cloud

A. Serviceübersicht

A.1. Der Symantec Web v2 Protect.cloud ("Web v2 Protect") Service untersucht Webseiten und Anhänge elektronisch auf Viren, bösartigen Code, Spyware und/oder Adware.

B. Servicemerkmale

B.1. Die externen HTTP- und FTP-over-HTTP-Anforderungen des Kunden, einschließlich aller Anhänge, Makros oder ausführbarer Dateien, werden über den Service geleitet.

B.2. Der Zugriff auf den Service ist über Scanning-IPs beschränkt (d. h. die IP-Adresse(n), von der/denen der Internetdatenverkehr des Kunden ausgeht). Die Scanning-IPs werden auch zur Identifizierung des Kunden und zur dynamischen Auswahl von kundenspezifischen Einstellungen verwendet.

B.3. Der Service scannt entsprechende Elemente der Webseite und ihrer Anhänge, die Viren, bösartigen Code, Spyware und/oder Adware enthalten können. Das Scannen bestimmter Webseiten, Inhalte oder Anhänge ist unter Umständen nicht möglich (zum Beispiel wenn sie mit einem Kennwort geschützt sind). Anhänge, die speziell als nicht scannfähig erkannt werden, werden nicht blockiert. Gestreamter und verschlüsselter Datenverkehr (d. h. Streaming-Medien und/oder HTTPS/SSL) kann nicht gescannt werden und durchläuft den Service ungescannt, es sei denn, der Kunde hat in der SMC HTTPS-Scans aktiviert.

B.4. Wenn auf einer Webseite, in einer Komponente einer Webseite oder in Anhängen ein Element als Virus, Spyware oder Adware identifiziert wird, wird der Zugang zu dieser Webseite oder einem Teilbereich dieser Webseite verweigert und der Benutzer wird automatisch zu einer Webseite mit einer Warnmeldung umgeleitet.

B.5. Der Roaming User Support ist eine optionale Funktion, die den Service auf Benutzer erweitert, die sich nicht innerhalb des Unternehmensnetzwerks befinden. Der Kunde muss eine PAC-Datei auf dem Benutzer-PC installieren, damit der Benutzer beim Starten des Browsers auf das Web-Portal des Service geleitet wird. Zum Zugriff auf das Web-Portal muss der Benutzer einen Benutzernamen und ein Kennwort eingeben. Eine Vorlage für die PAC-Datei kann von der SMC heruntergeladen und vom Kunden geändert werden.

C. Pflichten des Kunden

C.1. Der Kunde muss die Domänen angeben, die durch den Service geleitet werden. Die Konfiguration ist über die SMC vorzunehmen.

C.2. Der Kunde kann Einstellungen über die SMC konfigurieren. Falls keine Einstellungen konfiguriert werden, werden die Standardeinstellungen des Service übernommen.

C.3. Der Kunde ist dafür verantwortlich, dass interner HTTP/FTP-over-HTTP-Datenverkehr (beispielsweise in das Intranet des Unternehmens) nicht durch den Service geleitet wird.

C.4. Wenn der Kunde über Internetservices verfügt, die anstatt eines Proxy eine direkte Verbindung nutzen, ist der Kunde dafür verantwortlich, die notwendigen Änderungen an seiner eigenen Infrastruktur vorzunehmen, um die Ausführung des Service zu ermöglichen.

C.5. Der Kunde kann einen Bereich der automatischen Warnmeldungs-Webseiten über die SMC anpassen.

D. Berichterstattung

D.1. Die Berichterstattung über die Aktivitäten des Service erfolgt über die SMC.

D.2. Um die Berichterstattung über Benutzer oder Gruppen zu ermöglichen, muss der Kunde die hierfür erforderliche Servicesoftware ("Client Site Proxy") gemäß den Installationsrichtlinien für den Service installieren.

D.3. Detaillierte Berichtsdaten werden nur für einen Zeitraum von maximal vierzig (40) Tagen in der SMC gespeichert. Zusammenfassende Berichtsdaten sind für einen Zeitraum von maximal zwölf (12) Monaten verfügbar.

D.4. Der Kunde kann für die detaillierten Berichtsdaten einen verlängerten Berichterstellungszeitraum von bis zu sechs (6) Monaten separat erwerben.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Der Internetdatenverkehr des Kunden bei der Nutzung des Service darf dreißig Megabyte (30 MB) pro Benutzer und Kalendertag nicht überschreiten (berechnet als Durchschnitt pro Benutzer in Bezug auf die gesamte registrierte Nutzung für den Service). F.2. SYMANTEC ÜBERNIMMT KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE VIREN, BÖSARTIGEN CODE, SPYWARE ODER ADWARE NICHT ERKENNT.

Anhang 11 – Symantec Web v2 URL.cloud

A. Serviceübersicht

A.1. Der Symantec Web v2 URL.cloud ("Web v2 URL") Service ermöglicht die digitale Untersuchung von Webseiten und Anhängen basierend auf Konfigurationseinstellungen, die vom Kunden ausgewählt werden.

B. Servicebeschreibung

B.1. Die externen HTTP- und FTP-over-HTTP-Anforderungen des Kunden, einschließlich aller Anhänge, Makros oder ausführbarer Dateien, werden über den Service geleitet. HTTPS-Anforderungen werden vom Service gescannt, wenn der Kunde HTTPS-Scans in der SMC aktiviert.

B.2. Der Zugriff auf den Service ist über Scanning-IPs beschränkt (d. h. die IP-Adresse(n), von der/denen der Internetdatenverkehr des Kunden ausgeht). Die Scanning-IPs werden auch zur Identifizierung des Kunden und zur dynamischen Auswahl von kundenspezifischen Einstellungen verwendet.

B.3. Der Kunde kann den Service über die SMC konfigurieren, um granulare Richtlinienregeln festzulegen.

B.4. Wenn der Zugang zu einer Webseite des Kunden, einer Komponente einer Webseite oder zu Anhängen durch eine vom Kunden festgelegte Richtlinie eingeschränkt ist, wird der Zugriff auf diese Webseite oder einen Teilbereich dieser Webseite verweigert und der Benutzer wird automatisch zu einer Webseite mit einer Warnmeldung umgeleitet.

C. Pflichten des Kunden

C.1. Der Kunde kann Einstellungen über die SMC konfigurieren. Falls keine Einstellungen konfiguriert werden, werden die Standardeinstellungen des Service übernommen.

C.2. Der Kunde muss seinen externen Datenverkehr durch den Service leiten. Die Konfiguration ist über die SMC vorzunehmen.

C.3. Der Kunde muss sicherstellen, dass interner HTTP/FTP-over-HTTP-Datenverkehr (beispielsweise in das Intranet des Unternehmens) nicht durch den Service geleitet wird.

C.4. Wenn der Kunde über Internetservices verfügt, die anstatt eines Proxy eine direkte Verbindung nutzen, ist der Kunde dafür verantwortlich, die notwendigen Änderungen an seiner eigenen Infrastruktur vorzunehmen, um die Ausführung des Service zu ermöglichen.

C.5. Der Roaming User Support ist eine optionale Funktion, die den Service auf Benutzer erweitert, die sich nicht innerhalb des Unternehmensnetzwerks befinden. Der Kunde muss eine PAC-Datei auf dem Benutzer-PC installieren, damit der Benutzer beim Starten des Browsers auf das Web-Portal von Symantec geleitet wird. Zum Zugriff auf das Web-Portal muss der Benutzer einen Benutzernamen und ein Kennwort eingeben. Eine Vorlage für die PAC-Datei kann von der SMC heruntergeladen und vom Kunden geändert werden.

C.6. Der Kunde kann einen Bereich der automatischen Warnmeldungs-Webseiten über die SMC anpassen.

C.7. Der Internetdatenverkehr des Kunden bei der Nutzung des Service darf dreißig Megabyte (30 MB) pro Benutzer und Kalendertag nicht überschreiten (berechnet als Durchschnitt pro Benutzer in Bezug auf die gesamte registrierte Nutzung für den Web v2 URL.cloud Service). Für den Fall, dass dieser Tagesgrenzwert überschritten wird, behält sich Symantec folgende Maßnahmen vor:

- a) Verweigerung der Bereitstellung oder vorübergehende Einstellung des Service im Ganzen oder in Teilen mit sofortiger Wirkung bis zum Unterbleiben der übermäßigen Nutzung, oder
- b) Aufforderung des Kunden zum Erwerb eines zusätzlichen Nutzerkontingents entsprechend dem tatsächlichen Internetdatenverkehr des Kunden für die jeweilige Servicelaufzeit

D. Berichterstattung

D.1. Die Berichterstattung zu den Resultaten einer vom Kunden erstellten Richtlinienregel für Zugangsbeschränkungen erfolgt über die SMC.

D.2. Um die Verwaltung und Berichterstattung über Benutzer oder Gruppen zu ermöglichen, muss der Kunde die hierfür erforderliche Softwareanwendung für den Service ("Client Site Proxy") gemäß den Installationsrichtlinien für den Service installieren.

D.3. Detaillierte Berichtsdaten werden nur für einen Zeitraum von maximal vierzig (40) Tagen in der SMC gespeichert. Zusammenfassende Berichtsdaten sind für einen Zeitraum von maximal zwölf (12) Monaten verfügbar.

D.4. Der Kunde kann für die detaillierten Berichtsdaten einen verlängerten Berichterstellungszeitraum von bis zu sechs (6) Monaten separat erwerben.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. SYMANTEC ÜBERNIMMT KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE BLOCKIERTE URLS ODER BLOCKIERTE INHALTE NICHT ERKENNT.

Anhang 12 – Symantec Web v2 Smart Connect.cloud

A. Serviceübersicht

A.1. Der Symantec Web v2 Smart Connect.cloud ("SmartConnect") Service ermöglicht Benutzern, die nicht direkt mit dem Netzwerk verbunden sind, den Web v2 Protect.cloud Service oder Web v2 URL.cloud Service bzw. beide Services zu nutzen. Der Service kann nur von Kunden abonniert werden, die auch den Web v2 Protect.cloud und/oder Web v2 URL.cloud Service nutzen.

B. Servicemerkmale

B.1. Wenn der Benutzer in vertraglich festgelegten "Serviceländern" auf das Internet zugreift, werden die externen HTTP- und FTP-over-HTTP-Anfragen des Kunden, einschließlich aller Anhänge, Makros oder ausführbaren Dateien, über den Web v2 URL.cloud Service und Web v2 Protect.cloud Service (wie zutreffend) weitergeleitet. Die Umleitung erfolgt über die Servicesoftware ("Web Roaming Agent"). HTTPS-Anforderungen werden vom Service gescannt, wenn der Kunde HTTPS-Scans in der SMC aktiviert.

B.2. Der Zugriff auf den Web v2 URL.cloud Service und Web v2 Protect.cloud Service ist auf autorisierte Systeme, die über eine gültige Version der Servicesoftware verfügen, sowie auf autorisierte Benutzer, die für diese Services in der SMC aktiviert wurden, beschränkt. Die Servicesoftware und Informationen zu autorisierten Benutzern werden zur Identifizierung des Kunden und zur dynamischen Auswahl kundenspezifischer Einstellungen verwendet.

B.3. Die Richtlinienregeln für den Web v2 URL.cloud Service und Web v2 Protect.cloud Service gelten unabhängig davon, ob der Benutzer über ein konfiguriertes Netzwerkverzeichnis verbunden ist.

C. Pflichten des Kunden

C.1. Die Konfigurationseinstellungen, die zur Umleitung dieses externen Internetdatenverkehrs an die Servicesoftware sowie zur Weiterleitung des ausgehenden Datenverkehrs an den Web v2 URL.cloud Service und Web v2 Protect.cloud Service (wie zutreffend) erforderlich sind, werden vom Kunden vorgenommen und verwaltet.

C.2. Der Kunde muss eine PAC-Datei auf den jeweiligen Benutzer-PCs installieren, damit der Browser beim Starten an die Servicesoftware verwiesen wird. Eine Vorlage für die PAC-Datei kann von der SMC heruntergeladen und vom Kunden geändert werden.

C.3. Der Kunde ist dafür verantwortlich, dass interner HTTP/FTP-over-HTTP-Datenverkehr (beispielsweise in das Intranet des Unternehmens) nicht an die Servicesoftware verwiesen wird.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Kunden oder Partner sind nicht berechtigt und dürfen Dritte nicht autorisieren, die Kontrollgesetzen unterliegende Technologie direkt oder indirekt in eines der folgenden Länder zu verkaufen, weiterzuveräußern, zu exportieren, zu reexportieren, zu übertragen, umzuleiten, zu verteilen, zu entsorgen, offenzulegen oder anderweitig dort in Umlauf zu bringen: Afghanistan, Angola, Armenien, Aserbaidschan, Bosnien und Herzegowina, Burma, Burundi, China, Kuba, Demokratische Republik Kongo, Eritrea, Äthiopien, Iran, Irak, Nordkorea, Liberia, Libyen, Nigeria, Ruanda, Sierra Leone, Somalia, Sudan, Syrien, Tansania, Uganda und Zimbabwe.

F.2. Der Kunde ist nicht berechtigt, die Servicesoftware auf eine Drittpartei oder eine Einzelperson, die kein Mitarbeiter des Kunden ist, zu übertragen. Dazu gelten folgende Ausnahmen: (i) Der Kunde ist berechtigt, die Servicesoftware zur Nutzung im Auftrag des Kunden auf seine Vertragspartner zu übertragen oder das Herunterladen der Servicesoftware durch seine Vertragspartner zu dem vorgenannten Zweck zu ermöglichen, vorausgesetzt, dass der Kunde solche Drittparteien über deren Verpflichtungen in Bezug auf diesen Abschnitt unterrichtet.

F.3. Der Kunde erkennt an, dass in der Servicesoftware die Symantec-Standardeinstellungen festgelegt sind. Dies schließt ein, dass die notwendigen Anstrengungen unternommen werden, um den Internetdatenverkehr des Benutzers zu einem "optimalen" Zugriffspunkt in der Serviceinfrastruktur weiterzuleiten. Diese Weiterleitung basiert auf der Ermittlung des Standorts des Benutzers anhand einer IP-Adresse. Dies geschieht unabhängig von einer Bewertung der wahrscheinlichen Leistung des Internetzugangs des jeweiligen Endbenutzers und erfolgt nur für diejenigen Länder, deren Servicequalität Symantec als ausreichend erachtet.

F.4. Der Kunde erkennt an, dass Symantec für alle Länder außerhalb der geeigneten Serviceländer keine Serviceleistungen bereitstellt. Wenn Symantec feststellt, dass der Benutzer sich in einem Land befindet, bei dem es sich nicht um ein "Serviceland" handelt, steht der Service dem Benutzer nicht zur Verfügung. Eine aktuelle Liste der geeigneten Serviceländer ist auf folgender Website veröffentlicht: http://images.message-labs.com/EmailResources/ServiceAdminGuides/WebRoamingAgent/SmartConnect_NoServiceCountries.pdf.

F.5. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

Anhang 13 – Symantec Enterprise Vault.cloud

A. Serviceübersicht

A.1. Der Symantec Enterprise Vault.cloud ("EV.cloud") Service ist die Sammelbezeichnung für eine Reihe von Archivierungsservices und -optionen, die in diesem Anhang beschrieben werden. Kunden müssen jeden Service sowie Zusatzservices separat erwerben.

B. Servicemerkmale

B.1. Alle im Rahmen des Enterprise Vault.cloud Service bereitgestellten Services sind nur mit genehmigten Versionen von Mail-Servern und gehosteten E-Mail-Services kompatibel, die am Standort des Kunden installiert sind. Die Kompatibilitätsliste ist auf folgender Website veröffentlicht: <http://www.symantec.com/docs/TECH191408>.

B.2. Kunden können Daten aus dem Enterprise Vault Discovery.cloud Service exportieren. Für einen Aufpreis exportiert Symantec Daten aus Enterprise Vault.cloud und sendet sie per Kurierdienst an den Kunden. Auf Anfrage werden diese Daten dem Kunden verschlüsselt zugestellt.

B.3. Folgendes gilt sowohl für den Symantec Enterprise Vault Personal.cloud Service als auch für den Symantec Enterprise Vault Discovery.cloud Service:

- a) Die maximale Größe von E-Mails, die von Symantec Enterprise Vault Personal.cloud und Symantec Enterprise Vault Discovery.cloud aufgenommen werden können, beträgt 50 MB, sofern nichts anderes in diesem Anhang angegeben ist.
- b) Keiner der Services ist ein Ersatz dafür, dass der Kunde ein Backup seines Mail-Servers (bzw. seiner Mail-Server) erstellen sollte. Falls der Kunde einen Mail-Server wiederherstellen muss, sollte die Wiederherstellung mithilfe von Backup-Daten und nicht mithilfe der im Archiv gespeicherten Daten erfolgen.

B.4. Services und Optionen

B.4.1. Symantec Enterprise Vault Personal.cloud

Der Enterprise Vault Personal.cloud Service ist ein E-Mail-Archivierungsservice, der Benutzern Zugriff auf ihre eigenen persönlichen E-Mail-Archive gewährt.

- a) Der Service speichert und indexiert E-Mails und Anhänge sowie BlackBerry®-Nachrichten (SMS, PIN-zu-PIN-Nachrichten, Anrufprotokolle, wenn die Symantec Enterprise Vault.cloud BlackBerry® Option hinzugefügt wird) im Archiv.
- b) Benutzer können zudem über Microsoft Outlook® oder Microsoft Outlook® Web App (sofern unterstützt), IBM Lotus Notes®, BlackBerry®-Geräte und über eine browserbasierte sichere Website auf das Archiv zugreifen.

B.4.2. Symantec Enterprise Vault Discovery.cloud

Der Enterprise Vault Discovery.cloud Service ist ein E-Mail-Archivierungsservice, der Anfragen zu bestimmten Themen oder zur rechtlichen Offenlegung (E-Discovery) beschleunigt, Richtlinien zur E-Mail-Nutzung durchsetzt und Daten für bestimmte Zeiträume aufbewahrt, die der Kunde festlegt.

- a) Der Service speichert und indexiert E-Mails und Anhänge sowie BlackBerry®-Nachrichten (SMS, PIN-zu-PIN-Nachrichten, Anrufprotokolle, wenn die Symantec Enterprise Vault.cloud BlackBerry® Option hinzugefügt wird) im Archiv.
- b) Benutzer können über eine browserbasierte sichere Website auf das Archiv zugreifen.

B.4.3. Symantec Enterprise Vault.cloud BlackBerry® Option

Die Enterprise Vault.cloud BlackBerry® Option ist ein Zusatzservice für den Enterprise Vault Personal.cloud Service, mit dem Benutzer über ihre BlackBerry®-Geräte auf archivierte E-Mails, Anhänge, SMS- und PIN-zu-PIN-Nachrichten sowie Anrufprotokolle zugreifen und sie durchsuchen können. Die Enterprise Vault.cloud BlackBerry® Option kann von Administratoren über einen BlackBerry® Enterprise Server (BES) oder von Benutzern mithilfe des BlackBerry® Desktop Manager installiert werden. Für die BlackBerry® Option muss Servicesoftware heruntergeladen und installiert werden.

B.4.4. Symantec Enterprise Vault.cloud Import Option

Die Symantec Enterprise Vault.cloud Import Option ist ein Zusatzservice für den Enterprise Vault Personal.cloud oder Enterprise Vault Discovery.cloud Service, mit dem der Kunde vorhandene E-Mail-Altdaten in sein Archiv migrieren und integrieren kann. Mit diesem Zusatzservice kann der Kunde sowohl integrierte ältere E-Mails als auch neue E-Mail-Datenströme innerhalb des Archivs kombinieren.

- a) Dieser Zusatzservice erfordert die aktive Mitarbeit des Kunden bei der Planung, Analyse und Ausführung eines Integrationsplans.

- b) Für die Integration muss der Kunde E-Mail-Daten mit einem Kurierdienst an Symantec schicken. Sämtliche Daten sollten in verschlüsselter Form versendet werden und der Kunde muss nach Vorgaben von Symantec den Verschlüsselungscode bereitstellen.
- c) Der Kunde kann die Daten in einem kompatiblen Format aus unterstützten Repositorys extrahieren und bereitstellen.
- d) Nach Absprache mit dem Kunden weist dieser Zusatzservice jeder importierten E-Mail Benutzer zu. E-Mails, die keinem bestimmten Benutzer direkt zugewiesen werden können, werden in einem speziellen Postfach innerhalb des Archivs aufbewahrt.
- e) Sämtliche Migrationsaktivitäten können protokolliert und geprüft werden, um Informationsintegrität in den E-Mail-Datensätzen des Kunden herzustellen.
- f) Die maximale Größe von E-Mails, die aufgenommen werden können, beträgt 50 MB.
- g) Symantec kann keine Zusagen über die Zeitdauer machen, die für das Importieren der Daten nach ihrem Eingang bei Symantec benötigt wird.
- h) Symantec ist nicht dafür verantwortlich, wenn der Datenimport aufgrund einer Beschädigung der vom Kunden empfangenen Daten fehlschlägt.

B.4.5. Symantec Enterprise Vault.cloud for Box®

Symantec Enterprise Vault.cloud for Box® ist ein Zusatzservice für den Enterprise Vault Personal.cloud oder Enterprise Vault Discovery.cloud Service für Dateien, die in www.Box.com-Unternehmenskonten gespeichert sind. Mit diesem Zusatzservice können Kunden Box®-Benutzer nach E-Mail-Adressen dem Archiv zuweisen. Dieser Zusatzservice erfasst Dateien und überträgt sie sicher in Form von E-Mails in das Archiv. Dateien können anschließend während des E-Discovery-Prozesses oder für andere Zwecke durchsucht und abgerufen werden. Administratoren können Dateitypen in beliebiger Kombination auswählen.

B.4.6. Symantec Enterprise Vault.cloud for Salesforce Chatter®

Salesforce Chatter® ist ein Zusatzservice für Enterprise Vault.cloud. Symantec Enterprise Vault.cloud for Salesforce Chatter® ist ein Cloud-basierter Service, mit dem Beiträge aus Salesforce Chatter® archiviert werden können. Salesforce Chatter® erfasst und indiziert Salesforce Chatter®-Inhalte in Enterprise Vault Personal.cloud und Enterprise Vault Discovery.cloud. Der Kunde kann dann in Enterprise Vault Personal.cloud oder Enterprise Vault Discovery.cloud Inhalte direkt durchsuchen und Benutzer können aus Enterprise Vault Discovery.cloud Suchergebnisse für die weitere Überprüfung und Analyse exportieren.

B.4.7. Symantec Enterprise Vault.cloud for Microsoft SharePoint®

Symantec Enterprise Vault.cloud for Microsoft SharePoint® ist ein Cloud-basierter Service für die Archivierung von Dokumenten aus Microsoft SharePoint® Server vor Ort. Microsoft SharePoint® erfasst und indiziert SharePoint®-Inhalte in Enterprise Vault Discovery.cloud. Der Kunde kann dann in Enterprise Vault Discovery.cloud Inhalte direkt durchsuchen und Suchergebnisse für die weitere Überprüfung und Analyse exportieren. Microsoft SharePoint® ist ein Zusatzservice für Enterprise Vault Discovery.cloud.

B.4.8. Symantec Enterprise Vault.cloud Folder Sync Option

Die Symantec Enterprise Vault.cloud Folder Sync Option ist ein Zusatzservice für den Enterprise Vault Personal.cloud Service. Mithilfe dieser Option kann ein Kunde E-Mails im Enterprise Vault Personal.cloud Service ähnlich wie in der E-Mail-Struktur der Microsoft Outlook®-Ordner von Benutzern anzeigen. Wenn Benutzer E-Mails zwischen Microsoft Outlook®-Ordern verschieben und neue Microsoft Outlook®-Ordner erstellen bzw. deren Speicherort ändern, repliziert die Synchronisierungsfunktion anschließend diese Ordnerstruktur in Enterprise Vault Personal.cloud. Für die Folder Sync Option muss Servicesoftware heruntergeladen und installiert werden.

B.4.9. Symantec Enterprise Vault Mailbox Continuity.cloud

Symantec Enterprise Vault Mailbox Continuity.cloud ist ein Service, mit dem Benutzer über einen speziell eingerichteten Ordner in Microsoft Outlook® oder eine webbasierte Benutzeroberfläche während eines Ausfalls der E-Mail-Server-Hauptplattform ("Continuity-Ereignis") auf ihre E-Mails zugreifen können. Für die Nutzung dieses Service muss der Kunde mindestens einen der Symantec Email Security Services abonniert haben.

- a) Der Kunde stimmt zu, den Service in der SMC als Failover-Zustellungskanal zu konfigurieren und ferner Symantec den Zustellungsort (Mailhost-Name oder IP-Adresse) nach Domäne seiner E-Mail-Server zu Beginn dieses Service mitzuteilen. Der Kunde bestätigt und stimmt zu, dass es seine Pflicht ist, Symantec während seiner Nutzung des Service über Änderungen dieses Zustellungskanals zu informieren. Der Kunde bestätigt, dass das Unvermögen des Kunden, diese Konfigurationen durchzuführen oder diese Zustellinformationen an Symantec weiterzuleiten, negative Auswirkungen auf die Leistung des Service hat.
- b) FALLS SYMANTEC KEINE SMTP-VERBINDUNG MIT DEM KUNDEN HERSTELLEN KANN, WERDEN DIE E-MAILS DES KUNDEN IM AUFTRAG DES KUNDEN AUF DEN SERVICE

UMGELEITET. UM ALLE ZWEIFEL AUSZUSCHLIESSEN: (I) WENN DIE FIREWALL DES KUNDEN DIE FUNKTION EINES PROXY ÜBERNIMMT UND ANSTELLE DES E-MAIL-SERVERS ANTWORTET ODER (II) WENN DER E-MAIL-SERVER DES KUNDEN EINE ANTWORT AUSGIBT (EINSCHLIESSLICH, OHNE DARAUF BESCHRÄNKT ZU SEIN, FEHLERCODES), DANN GILT DIES ALS EINE SMTP-VERBINDUNG UND WIRD NICHT ALS CONTINUITY-EREIGNIS GEWERTET.

- c) Der Service verwendet eine opportunistische TLS-Verbindung bei der E-Mail-Zustellung. SÄMTLICHE EMAIL BOUNDARY ENCRYPTION.CLOUD- UND POLICY BASED ENCRYPTION.CLOUD-KUNDEN, DIE ZUSÄTZLICH DEN SERVICE ABONNIEREN, BESTÄTIGEN UND STIMMEN ZU, DASS VERSUCHT WIRD, EINE TLS-VERBINDUNG HERZUSTELLEN, EINE HERSTELLUNG EINER SOLCHEN VERBINDUNG JEDOCH GGF. NICHT MÖGLICH IST UND E-MAILS AUS DIESEM GRUND EVENTUELL NICHT VERSCHLÜSSELT WERDEN. DER KUNDE ERKENNT AN UND STIMMT ZU, DASS ER KEINE VERTRAULICHEN E-MAILS ÜBER DEN SERVICE SENDEN ODER EMPFANGEN SOLLTE UND EIN SENDEN BZW. EMPFANGEN SOLCHER E-MAILS AUSSCHLIESSLICH AUF EIGENES RISIKO DES KUNDEN ERFOLGT.
- d) Während der Laufzeit des Service werden alle vom Service abgerufenen oder gespeicherten E-Mails neunzig (90) Tage lang gespeichert und können vom Kunden abgerufen werden. Nach Ablauf dieser Frist werden sie automatisch gelöscht.
- e) Der Kunde erkennt an und stimmt zu, dass, (i) die Symantec Email Security Services nicht alle E-Mails scannen, die ursprünglich im Archiv eingehen, und (ii) die Scan-Services von Symantec (Email AntiVirus.cloud, Email AntiSpam.cloud, Email Image Control.cloud und Email Data Protection.cloud) keine E-Mails scannen, die aus dem Archiv für eine Wiederherstellung in den Benutzerpostfächern freigegeben werden. Dementsprechend übernimmt Symantec keine Haftung für Viren, Spam, Bilder oder unangemessene Inhalte, die in solchen wiederhergestellten E-Mails enthalten sein können. Darüber hinaus findet das Service Level Agreement auf diese wiederhergestellten E-Mails keine Anwendung.

B.4.10. Symantec Enterprise Vault.cloud IM Logging Option

Die Symantec Enterprise Vault.cloud IM Logging Option kann nur von Kunden abonniert werden, die auch den Symantec Instant Messaging Security.cloud Service nutzen. Die IM Logging Option ist ein Zusatzservice für den Symantec Instant Messaging Security.cloud Service. Die IM Logging Option archiviert mithilfe des Enterprise Vault.cloud Service Mitschriften von Instant Messages aus Symantec Instant Messaging Security.cloud. Die IM Logging Option erfasst und indexiert Instant Messaging-Mitschriften in Enterprise Vault Discovery.cloud. Der Kunde kann dann in Enterprise Vault Discovery.cloud Inhalte direkt durchsuchen und Suchergebnisse für die weitere Überprüfung und Analyse exportieren.

C. Pflichten des Kunden.

C.1. Der Kunde muss jeden Service konfigurieren (wie zutreffend).

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support.

E.1. Der Kunde kann den aktuellen Systemstatus des Service online anzeigen.

E.2. Der Kunde hat Zugang zu einer Selbstbedienungshilfe und Supportdatenbank für den Service.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. Sämtliche von Symantec oder deren Drittanbietern im Rahmen dieses Service gespeicherten oder archivierten Kundendaten sind alleiniges Eigentum des Kunden ("Kundendaten"). Keine der in diesem Dokument enthaltenen Bestimmungen überträgt Symantec oder deren Anbietern irgendwelche gesetzlichen oder billigkeitsrechtlichen Rechte, Titel oder Interessensansprüche an den Kundendaten.

F.2. Die Kundendaten werden während der Laufzeit des Service archiviert. Vor Ablauf der Servicelaufzeit oder bei Kündigung des Service kann der Kunde Symantec schriftlich auffordern: (i) die Kundendaten zu löschen, ohne dass zusätzliche Kosten anfallen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist); oder (ii) dem Kunden eine Offline-Kopie im PST-Format auf Festplatte zuzustellen, wobei hierfür die zu diesem Zeitpunkt gültigen Gebühren von Symantec gelten. Falls der Kunde Symantec keine wie im vorangehenden Satz beschriebene schriftliche Anweisung zukommen lässt, ist Symantec berechtigt, die Kundendaten zu löschen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist).

F.3. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

Anhang 14 – AdvisorMail on Symantec.cloud

A. Serviceübersicht

A.1. AdvisorMail on Symantec.cloud™ ("AdvisorMail") ist ein Service für die E-Mail-Archivierung und -Compliance. Kunden müssen den Service sowie Zusatzservices separat erwerben.

B. Servicemerkmale

B.1. AdvisorMail on Symantec.cloud™

Nachrichten werden in Übereinstimmung mit den Richtlinien des Kunden erfasst, gespeichert und indexiert sowie automatisch gescannt und gekennzeichnet. E-Mails oder Anhänge, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann nach Bedarf vom Kunden geprüft werden.

B.2. AdvisorMail IM Option on Symantec.cloud™

AdvisorMail IM Option on Symantec.cloud™ ist ein Zusatzservice für den AdvisorMail on Symantec.cloud Service für unterstützte Instant Messaging-Plattformen. Instant Messages werden in Übereinstimmung mit den Richtlinien des Kunden erfasst, gespeichert und indexiert sowie automatisch gescannt und gekennzeichnet. Instant Messages, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann nach Bedarf vom Kunden geprüft werden. AdvisorMail IM Option on Symantec.cloud™ arbeitet mit unterstützten Instant Messaging-Netzwerken und -Clients zusammen, die aktuell in der Kompatibilitätsliste für die AdvisorMail IM Option auf folgender Website definiert sind:

<http://archive.onconfluence.com/display/~ptath/Supportive+IMs+and+Proxy+Settings>.

B.3. AdvisorMail Bloomberg Option on Symantec.cloud™

Die AdvisorMail Bloomberg Option on Symantec.cloud™ ist ein Zusatzservice für den AdvisorMail on Symantec.cloud Service für Instant Bloomberg® (Instant Messages) und Bloomberg®-E-Mail. Bloomberg®-Nachrichten werden in Übereinstimmung mit den Richtlinien des Kunden erfasst, gespeichert und indexiert sowie automatisch gescannt und gekennzeichnet. Dieser Zusatzservice zeichnet Instant Bloomberg®-Nachrichten und Bloomberg®-E-Mails in AdvisorMail on Symantec.cloud in ihrem systemeigenen Format auf. Bloomberg®-Nachrichten, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann nach Bedarf vom Kunden geprüft werden.

B.4. Symantec Enterprise Vault.cloud Import Option

Die Symantec Enterprise Vault.cloud Import Option ist ein Zusatzservice für den AdvisorMail on Symantec.cloud Service, mit dem der Kunde vorhandene E-Mail-Altdaten in sein Archiv migrieren und integrieren kann. Mit diesem Zusatzservice kann der Kunde sowohl integrierte ältere E-Mails als auch neue E-Mail-Datenströme innerhalb des Archivs kombinieren.

- a) Dieser Zusatzservice erfordert die aktive Mitarbeit des Kunden bei der Planung, Analyse und Ausführung eines Integrationsplans.
- b) Für die Integration muss der Kunde E-Mail-Daten mit einem Kurierdienst an Symantec schicken. Sämtliche Daten sollten in verschlüsselter Form versendet werden und der Kunde muss nach Vorgaben von Symantec den Verschlüsselungscode bereitstellen.
- c) Der Kunde kann die Daten in den Formaten, die in der Kompatibilitätsliste definiert sind, aus unterstützten Repositories extrahieren und bereitstellen.
- d) Nach Absprache mit dem Kunden weist dieser Zusatzservice jeder importierten E-Mail Benutzer zu. E-Mails, die keinem bestimmten Benutzer direkt zugewiesen werden können, werden in einem speziellen Postfach innerhalb des Archivs aufbewahrt.
- e) Sämtliche Migrationsaktivitäten können protokolliert und geprüft werden, um Informationsintegrität in den E-Mail-Datensätzen des Kunden herzustellen.
- f) Die maximale Größe von E-Mails, die aufgenommen werden können, beträgt 50 MB.
- g) Symantec kann keine Zusagen über die Zeitdauer machen, die für das Importieren der Daten nach ihrem Eingang bei Symantec benötigt wird.
- h) Symantec ist nicht dafür verantwortlich, wenn der Datenimport aufgrund einer Beschädigung der vom Kunden empfangenen Daten fehlschlägt.

C. Pflichten des Kunden.

C.1. Der Kunde muss jeden Service konfigurieren (wie zutreffend).

D. **Berichterstattung.** Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. **Technischer Support.**

E.1. Technischer Support wird rund um die Uhr (24x7) per Telefon oder online bereitgestellt.

E.2. Der Kunde kann den aktuellen Systemstatus des Service auf folgender Website einsehen:
<http://support.liveoffice.com/system-status/lax>.

E.3. Der Kunde hat Zugang zu einer Selbstbedienungshilfe und Supportdatenbank für den Service.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. Sämtliche von Symantec oder seinen Drittanbietern im Rahmen dieser Vereinbarung gespeicherten oder archivierten Kundendaten sind alleiniges Eigentum des Kunden ("Kundendaten"). Keine der in diesem Anhang enthaltenen Bestimmungen überträgt Symantec oder deren Anbietern irgendwelche gesetzlichen oder billigungsrechtlichen Rechte, Titel oder Interessensansprüche an den Kundendaten.

F.2. Die Kundendaten werden während der Laufzeit des Service archiviert. Vor Ablauf der Servicelaufzeit oder bei Kündigung des Service kann der Kunde Symantec schriftlich auffordern: (i) die Kundendaten zu löschen, ohne dass zusätzliche Kosten anfallen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist); oder (ii) dem Kunden eine Offline-Kopie im PST-Format auf Festplatte zuzustellen, wobei hierfür die zu diesem Zeitpunkt gültigen Gebühren von Symantec gelten. Falls der Kunde Symantec keine wie im vorangehenden Satz beschriebene schriftliche Anweisung zukommen lässt, ist Symantec berechtigt, die Kundendaten zu löschen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist).

F.3. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

Anhang 15 – Symantec Email Continuity Archive.cloud und Symantec Email Continuity Archive Lite.cloud

A. Serviceübersicht

A.1. Der Symantec Email Continuity Archive.cloud und Symantec Email Continuity Archive Lite.cloud Service sind gehostete E-Mail-Speicherungssysteme, mit denen die Systemadministratoren des Kunden bestimmte E-Mail-Aufbewahrungsrichtlinien für die Speicherung archivierter E-Mails für eine bestimmte Gruppe von E-Mail-Postfächern festlegen können.

B. Servicemerkmale

B.1. Der **Symantec Email Continuity Archive.cloud Service** umfasst die folgenden Servicemerkmale:

- a) E-Mail-Erfassung und -Speicherung: E-Mails werden erfasst, sobald sie der primären E-Mail-Umgebung des Kunden zugestellt und in ein E-Mail-Archiv übertragen werden, um indexiert und gespeichert zu werden. E-Mails werden im Service verschlüsselt und gespeichert. E-Mail-Aufbewahrungsrichtlinien können für Benutzer festgelegt werden, um zu bestimmen, wann E-Mails aus dem Service zu löschen sind.
- b) Wiederherstellung: Bietet die Möglichkeit zur Wiederherstellung von E-Mails aus dem E-Mail-Archiv zurück in die Exchange-Nachrichtenspeicher des Kunden.
- c) E-Discovery: Bietet den Systemadministratoren des Kunden die Möglichkeit, bestimmte Benutzer als "Prüfer" zu bestimmen und ihnen die Möglichkeit zu geben, zu E-Discovery-Zwecken (Auffinden elektronisch gespeicherter Daten) sowie zu anderen Zwecken neben ihren eigenen auch E-Mails in anderen Postfächern zu überprüfen. Die Prüfer können ein Discovery-Archiv anlegen, das die Ergebnisse einer Suche in Benutzerpostfächern enthält. Das Discovery-Archiv kann in ein einzelnes Postfach exportiert werden.
- d) Windows-Authentifizierung: Ermöglicht Kunden, die Microsoft Exchange® 2000, Microsoft Exchange® 2003 und/oder Microsoft Exchange® 2007 nutzen, die Sicherheitsrichtlinien des Kunden für die Microsoft Active Directory-Authentifizierung auf Benutzer des Service auszuweiten, indem Benutzern die Möglichkeit gegeben wird, sich mittels ihres Active Directory-Kennworts beim Service einzuloggen.
- e) Endbenutzerarchiv: Ermöglicht von einer Aufbewahrungsrichtlinie erfassten Benutzern, von ihrem Postfach aus über eine webbasierte Oberfläche auf ihr persönliches Archiv zuzugreifen, in dem E-Mails gespeichert sind. Die E-Mail-Administratoren des Kunden können auch festlegen, ob Benutzer E-Mails von ihrem persönlichen Archiv aus weiterleiten können oder nicht.
- f) Speicherverwaltung: Die Systemadministratoren des Kunden können eine Speicherungsverwaltungsrichtlinie definieren, mit der Anhänge aus den Exchange-Nachrichtenspeichern des Kunden in den Service verschoben werden können

B.2. Der **Symantec Email Continuity Archive Lite.cloud Service** umfasst folgende Servicemerkmale (wie oben näher beschrieben):

- a) E-Mail-Erfassung und -Speicherung
- b) Wiederherstellung
- c) E-Discovery
- d) Windows-Authentifizierung

Der Symantec Email Continuity Archive Lite.cloud Service umfasst nicht die folgenden Servicefunktionen: Endbenutzerarchiv und Speicherverwaltung. Der Kunde kann auf die Endbenutzerarchiv-Servicefunktion aufrüsten, indem er das Symantec Email Continuity Archive Lite.cloud End User Pack abonniert.

B.3. Data Import Option.

Der Kunde ist berechtigt, Altdaten aus PST-Dateien in den Service zu importieren, indem er ein Import-Tool herunterlädt und verwendet. Dafür ist die Entrichtung einer Importgebühr basierend auf der Menge der zu importierenden Daten notwendig. Für den Fall, dass die tatsächliche Menge Altdaten die Menge der erworbenen Importdaten übersteigt, behält Symantec sich das Recht vor, die für diese zusätzlichen Daten entstehenden Kosten zu den dann geltenden Preisen in Rechnung zu stellen.

B.4. Symantec Email Continuity.cloud Storage Option

- a) Der Speicher des Kunden wird nach der Rohdatenmenge der E-Mails, die in den Service übertragen und im Service gespeichert werden, bemessen.
- b) Falls der Kunde die Pakete Symantec Complete Email Safeguard.cloud, Symantec Complete Email & Web Safeguard.cloud oder Symantec Ultimate Safeguard.cloud abonniert,

- c) enthält das Paket für die Services Symantec Email Continuity.cloud und Symantec Email Continuity Archive.cloud zusammen neuen E-Mail-Speicherplatz von maximal 0,7 GB pro Benutzer pro Jahr. Sollte der Kunde sein Speicherkontingent überschreiten, stellt Symantec zusätzlich genutzten Speicherplatz zu den dann geltenden Tarifen in Rechnung.

B.5. Ablauf des Service und Datenextrahierung

B.5.1. Bei Kündigung des Symantec Email Continuity Archive.cloud oder Symantec Email Continuity Archive Lite.cloud Service löscht Symantec die Daten des Kunden aus dem Archiv.

B.5.2. Der Kunde kann jederzeit vor Ablauf des Service seine Daten aus dem Archiv extrahieren.

C. Pflichten des Kunden

C.1. Der Kunde ist für folgende Maßnahmen in Bezug auf den Service zuständig:

- a) Bereitstellen und Warten der notwendigen Hardware und Software (gemäß den Angaben im Bereitstellungsformular)
- b) Sicherstellen, dass ein zuständiger technischer Mitarbeiter mit Administratorrechten zur Bereitstellung des Service zur Verfügung steht
- c) Festlegen, welche Benutzer zum Empfang des Service berechtigt sein sollen, sowie des vorgegebenen Aufbewahrungszeitraums für jeden dieser Benutzer
- d) Festlegen und Schützen von Berechtigungen für den Zugriff auf das Archiv über die Kundenschnittstelle
- e) Festlegen und Verwalten von Archivierungsaufbewahrungsrichtlinien
- f) Durchführen von Suchvorgängen für den Abruf archivierter Daten

C.2. Falls der Kunde die zur Bereitstellung des Service erforderlichen Maßnahmen nicht innerhalb von dreißig (30) Tagen ab dem Datum der Kundenbestellung durchgeführt hat, kann Symantec nach Ablauf dieser Frist damit beginnen, Kosten für den Service in Rechnung zu stellen.

C.3. Die oben beschriebenen Pakete enthalten keine Speicherkapazität für den Altdatenimport. Der Kunde ist daher verpflichtet, ausreichend zusätzlichen Speicherplatz zu erwerben, um diese Anforderungen zu erfüllen.

C.4. Falls der Kunde nicht eines der oben aufgeführten Pakete abonniert, umfasst der Preis pro Benutzer keinen Speicherplatz und der Kunde muss ausreichend großen Speicherplatz für den Service erwerben.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. KEIN E-MAIL-ARCHIVIERUNGSSERVICE KANN EINE 100-PROZENTIGE GENAUIGKEIT GARANTIEREN. DESHALB ÜBERNIMMT SYMANTEC KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT AUF SERVICEAUSFÄLLE ZURÜCKZUFÜHREN SIND. DAVON UNBERÜHRT BLEIBEN DIE RECHTSMITTEL, DIE IM SERVICE LEVEL AGREEMENT IN ANLAGE 3 AUSDRÜCKLICH VORGESEHEN SIND.

F.2. Symantec übernimmt keine Haftung, falls der Service eventuell nicht gemäß der Beschreibung in diesem Anhang bereitgestellt wird, was dadurch verursacht werden kann, dass (i) Symantec nicht seine Standardpraktiken bei der Bereitstellung und Verwaltung des Service für den Kunden anwenden kann, (ii) der Kunde die im Benutzerhandbuch oder Bereitstellungsformular dargelegten Symantec-Richtlinien nicht befolgt oder (iii) der Kunde es versäumt, den Service zu aktivieren oder nutzen.

F.3. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

F.4. Der Kunde erkennt an und stimmt zu, dass, (i) die Scan-Services von Symantec (Email AntiVirus.cloud, Email AntiSpam.cloud, Email Image Control.cloud und Email Data Protection.cloud) nicht alle E-Mails scannen, die ursprünglich im Archiv eingehen, und (ii) die Scan-Services von Symantec (Email AntiVirus.cloud, Email AntiSpam.cloud, Email Image Control.cloud und Email Data Protection.cloud) keine E-Mails scannen, die aus dem Archiv für eine Wiederherstellung in den Benutzerpostfächern freigegeben werden. Dementsprechend übernimmt Symantec keine Haftung für Viren, Spam, Bilder oder unangemessene Inhalte, die in solchen wiederhergestellten E-Mails enthalten sein können. Darüber hinaus findet das Service Level Agreement auf diese wiederhergestellten E-Mails keine Anwendung.

F.5. Der Kunde bestätigt und stimmt zu, dass Symantec unter keinen Umständen die Funktion eines Drittanbieter-Downloaders im Sinne der SEC-Bestimmungen übernehmen kann.

Anhang 16 – Symantec Email Continuity.cloud

A. Serviceübersicht

A.1. Der Symantec Email Continuity.cloud ("EC") Service ist ein Standby-Nachrichtenaustauschsystem für die Umgebungen Microsoft Exchange® und Lotus Notes®.

B. Servicemerkmale

B.1. Email Continuity.cloud synchronisiert wichtige System- und Nutzerdaten, unter anderem das E-Mail-Verzeichnis und die persönlichen Kontakte einzelner Benutzer. Der Kunde kann Email Continuity.cloud darüber hinaus für die Unterstützung von BlackBerry®-Geräten mittels drahtloser Weiterleitung unter Verwendung des BlackBerry® Web Client oder BlackBerry® Internet Service sowie für die Integration in Microsoft Outlook® für Benutzer des Cached Mode in Outlook® 2003 oder Outlook® 2007 über eine installierte Outlook-Erweiterung einrichten.

B.2. Unterstützte Versionen: Microsoft Exchange® 5.5, Microsoft Exchange® 2000, Microsoft Exchange® 2003, Microsoft Exchange® 2007, Lotus Notes® Version 6, Lotus Notes® Version 7.

B.3. Unterstützte Versionen für Microsoft Outlook®-Erweiterung: Microsoft Outlook® 2003 im Cached Mode; Microsoft Outlook® 2007 im Cached Mode.

B.4. Aktivierung: Der Kunde kann die Aktivierung von Email Continuity.cloud telefonisch beim Kundendienst von Symantec oder über das SMC anfordern. Nach Aktivierung von Email Continuity.cloud erhält der Kunde per SMS Benachrichtigungen an von ihm genannte Mobiltelefone und persönliche E-Mail-Adressen. Zu diesem Zeitpunkt beginnt Email Continuity.cloud, eingehende E-Mails zu empfangen und zu sortieren, sie (vorbehaltlich Absatz F.1 unten) gegebenenfalls entsprechend anderen vom Kunden abonnierten E-Mail-Services von Symantec (z. B. Email AntiVirus.cloud Service) zu filtern und an die entsprechenden Benutzerpostfächer weiterzuleiten. Email Continuity.cloud sorgt für bis zu dreißig (30) Tage nach der Deaktivierung für die Speicherung und Aufbewahrung von während der Aktivierung gesendetem und empfangenem E-Mail-Verkehr.

B.5. Aufbewahrung: Der Kunde ist für die Festlegung der Benutzer, deren E-Mails aufbewahrt werden sollen, sowie des anzugebenden Aufbewahrungszeitraums für jeden dieser Benutzer verantwortlich. Die aufbewahrten E-Mails werden (i) nach Ablauf des festgelegten Aufbewahrungszeitraums für diese Benutzer oder (ii) nach Kündigung von Email Continuity.cloud gelöscht; maßgeblich ist dabei der zuerst eintretende Fall.

B.6. Authentication Manager: Der Kunde kann seine Sicherheitsrichtlinien für die Authentifizierung durch Microsoft Active Directory auf Email Continuity.cloud erweitern, indem er es Benutzern ermöglicht, sich mit ihren Windows-Kennwörtern bei ihren Email Continuity.cloud-Postfächern anzumelden, so dass die Notwendigkeit eines gesonderten Email Continuity.cloud-Kennworts entfällt. Die Windows-Authentifizierung setzt die Verfügbarkeit eines zum Zeitpunkt der Aktivierung von Email Continuity.cloud für den Authentication Manager zugänglichen Windows-Domänencontrollers voraus, der zur Authentifizierung von Benutzern bei der Anmeldung an Email Continuity.cloud-Postfächern in der Lage ist. Unterstützte Versionen: Microsoft Exchange® 2000, Microsoft Exchange® 2003, Microsoft Exchange® 2007

B.7. Das vom Kunden zu erwerbende Mindestkontingent an Email Continuity.cloud-Benutzern beläuft sich (i) auf eine Anzahl von Benutzern, die der Anzahl der Postfächer in der Microsoft Exchange® -Umgebung des Kunden entspricht, oder (ii) auf zehn (10) Benutzer, wobei die jeweils größere Anzahl ausschlaggebend ist.

B.8. Teilaktivierung: Bei bestimmten E-Mail-Systemen/-Versionen (z. B. Microsoft Exchange® 2000-, 2003- und 2007-Umgebungen) kann Email Continuity.cloud für Teilbereiche der Umgebung des Kunden aktiviert werden (eine oder mehrere Personen, ein oder mehrere Server und/oder ein oder mehrere Standorte); durch eine solche Teilaktivierung können örtlich begrenzte E-Mail-Ausfälle abgefangen werden.

B.9. Aktivierung: Ein Abonnement von Email Continuity.cloud berechtigt den Kunden zu vierundzwanzig (24) Aktivierungsvorgängen pro Jahr für einen Zeitraum von jeweils bis zu zwölf (12) aufeinanderfolgenden Stunden ("inbegriffene Aktivierungen"). Der Kunde kann zusätzliche Aktivierungen (für einen Zeitraum von jeweils zwölf (12) aufeinanderfolgenden Stunden) zu den zum betreffenden Zeitpunkt geltenden Tarifen von Symantec erwerben.

B.10. Systemtests: Die Systemtests umfassen (i) pro Vierteljahr einen (1) Test von Email Continuity.cloud für alle Benutzer mit einer Dauer von bis zu vier (4) Stunden sowie (ii) für Microsoft Exchange® 2000-, Microsoft Exchange® 2003- oder Microsoft Exchange® 2007-Umgebungen unbegrenzte Teilstests für bis zu zehn Prozent (10 %) der Benutzer. Der Kunde muss den Termin für diese Tests mindestens sieben (7) Geschäftstage vor dem vom Kunden gewünschten Testdatum mit Symantec abstimmen.

B.11. Falls der Kunde die Services Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Data Protection.cloud und/oder Email Image Control.cloud nutzt, kann Symantec das Failover-Routing für die E-Mails des Kunden in

die Email Continuity.cloud-Umgebung innerhalb der SMC konfigurieren. Dieses Failover-Routing wird verwendet, wenn der Email Continuity.cloud Service aktiviert ist.

B.12. Optionen

B.12.1. Symantec Email Continuity – .cloud Storage Option

- a) Falls der Kunde eines der Pakete Symantec Complete Email Safeguard.cloud, Symantec Complete Email & Web Safeguard.cloud oder Symantec Ultimate Safeguard.cloud abonniert, enthält das Paket für die Services Symantec Email Continuity.cloud und Symantec Email Continuity Archive.cloud insgesamt maximal 0,7 GB neuen E-Mail-Speicherplatz pro Benutzer pro Jahr. Sollte der Kunde sein Speicherkontingent überschreiten, stellt Symantec zusätzlich genutzten Speicherplatz zu den dann geltenden Tarifen in Rechnung.
- b) Falls der Kunde nicht eines der oben in Absatz B.12.1.a aufgeführten Pakete abonniert, umfasst der Preis pro Benutzer keinen Speicherplatz, und der Kunde muss ausreichend großen Speicherplatz für den Service erwerben.

B.12.2. Symantec Email Continuity – .cloud Wireless Option

- a) Wenn der Kunde die Option Symantec Email Continuity.cloud Wireless Option abonniert, können Systemadministratoren bestimmte BlackBerry®-Geräte unter Verwaltung durch RIM BlackBerry® Enterprise Server (BES) bereitstellen. Wenn Email Continuity.cloud aktiviert ist, erfolgt das Senden und Empfangen von E-Mails durch BlackBerry®-Geräte weiterhin im Datenaustausch mit EMS, und zwar über einen vom BES-Server eingerichteten sicheren Kanal.
- b) Unterstützte Versionen: Microsoft Exchange® 2000, Microsoft Exchange® 2003 oder Microsoft Exchange® 2007; BlackBerry® Enterprise Server ab Version 4.0; BlackBerry® Handheld-Geräte ab Firmwareversion 4.1.

C. Pflichten des Kunden

C.1. Der Kunde ist dafür verantwortlich, die erforderliche Hardware und Software (wie im Bereitstellungsformular angegeben) bereitzustellen und zu verwalten.

C.2. Der Kunde muss zu Aufbewahrungszwecken ausreichend großen Speicherplatz erwerben.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass die vom Kunden abonnierten Scan-Services von Symantec für eingehende und ausgehende E-Mails umgangen werden, wenn sich der Kunde in einem aktivierten Zustand befindet und der Kunde daraufhin E-Mails an eine andere, ebenfalls in einem aktivierten Zustand befindliche Organisation sendet oder von dieser empfängt.

F.2. Falls der Kunde die Services Email AntiVirus.cloud, Email AntiSpam.Cloud, Email Data Protection.cloud oder Email Image Control.cloud nicht nutzt, liegt es in der Verantwortung des Kunden, das Failover-Routing für die E-Mails des Kunden an die Email Continuity.cloud-Umgebung zu konfigurieren und zu testen. Diese Failover müssen im Rahmen des Bereitstellungsprozesses entsprechend den Anweisungen von Symantec eingerichtet und danach aufrechterhalten werden. Sollte der Kunde es versäumen, diese Failover einzurichten oder aufrechtzuerhalten, nimmt der Kunde zur Kenntnis und akzeptiert, dass E-Mails nicht an Email Continuity.cloud weitergeleitet werden können.

F.3. SYMANTEC HAFTET NICHT FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS DER SERVICE E-MAIL-SYSTEME NICHT SYNCHRONISIERT.

Anhang 17 – Symantec Email Archiving.cloud P

A. Serviceübersicht

A.1. Bei den Services Symantec Email Archiving.cloud (P), Symantec Email Archiving.cloud Lite (P) und Symantec Email Archiving.cloud Premium (P) (zusammen als "Archiving.cloud (P) Service" bezeichnet) handelt es sich um hybride Managed Services für das Archivieren, Speichern und Abrufen von E-Mails.

B. Servicemerkmale

B.1. Symantec kontaktiert den Kunden, um einen Termin für eine anfängliche Telekonferenz zu vereinbaren.

B.2. Diese anfängliche Telekonferenz findet über WebEx statt®. Bei diesem Gespräch werden von den Parteien folgende Aktionen durchgeführt:

- a) Überprüfen, dass alle Aktionen gemäß der Setup-Anleitung (Client Setup Document) ausgeführt wurden
- b) Installieren der Archivierungs- und sonstiger Software mittels des aktuellen Symantec-Dokuments über Archivierungsinstallationsverfahren
- c) Überprüfen der Active Directory-Einstellungen
- d) Aktivieren des Service
- e) Überprüfung der Verfügbarkeit der Benutzeroberfläche
- f) Überprüfen der Archivierung (Site-to-Site)
- g) Erstellen von Kopien der Verschlüsselungscodes gemäß dem aktuellen Symantec-Dokument über Codesicherungsverfahren

B.3. Eine Schulungssitzung kann während oder nach der anfänglichen Telekonferenz in Anspruch genommen werden und umfasst Sitzungen, die sich auf folgende Themen konzentrieren: (i) IT, (ii) Richtlinien, (iii) Überwachung und (iv) Endbenutzer.

B.4. Ungefähr eine (1) Woche nach der Aktivierung wird eine Telekonferenz für die abschließende Überprüfung ("Post-Review") angesetzt. Nach diesem Post-Review-Gespräch kann der Kunde für weitere Hilfe die Standardverfahren für technischen Support in Anspruch nehmen.

B.5. Für Kunden mit *bis zu 500 Benutzern* umfasst der Symantec Email Archiving.cloud Lite (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) 3-jährige Aufbewahrungszeit
- c) Maximaler Speicherplatz von 3 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.6. Für Kunden mit *mehr als 500 Benutzern* umfasst der Symantec Email Archiving.cloud Lite (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) 1-jährige Aufbewahrungszeit
- c) Maximaler Speicherplatz von 1,5 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.7. Für Kunden mit *bis zu 500 Benutzern* umfasst der Symantec Email Archiving.cloud (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) 10-jährige Aufbewahrungszeit
- c) Maximaler Speicherplatz von 10 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.8. Für Kunden mit *mehr als 500 Benutzern* umfasst der Symantec Email Archiving.cloud (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) Unbegrenzte Aufbewahrungszeit
- c) Maximaler Speicherplatz von 6 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.9. Für Kunden mit *bis zu 500 Benutzern* umfasst der Symantec Email Archiving.cloud Premium (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) Premium-Funktionen gemäß der Beschreibung in Absatz B.12. unten
- c) 10-jährige Aufbewahrungszeit
- d) Maximaler Speicherplatz von 10 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.10. Für Kunden mit *mehr als 500 Benutzern* umfasst der Symantec Email Archiving.cloud Premium (P) Service Folgendes:

- a) Standardfunktionen gemäß der Beschreibung in Absatz B.11. unten
- b) Premium-Funktionen gemäß der Beschreibung in Absatz B.12. unten
- c) Unbegrenzte Aufbewahrungszeit
- d) Maximaler Speicherplatz von 6 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl)

B.11. Standardfunktionen

B.11.1. Adressauflösung und Verteilerliste/Gruppenerweiterung. Alle von Exchange als interne Adressen markierten E-Mail-Adressen werden im entsprechenden Benutzerpostfach aufgelöst. Für jede Verteilerliste, die als Empfänger der Nachricht referenziert ist, wird eine Liste mit zu dem Zeitpunkt aktuellen Mitgliedschaftsinformationen in Form zusätzlicher Metadaten zur E-Mail-Nachricht erfasst.

B.11.2. Volltextindex. Die E-Mail-Archivierungs-Appliance kann Textinhalte aus verschiedenen Anhangstypen sowie gemeinsamen Feldern in der Nachricht extrahieren, um die Erstellung eines Volltextindexes für Suchen innerhalb des Archiving.cloud (P) Service zu unterstützen.

B.11.3. Verschlüsselung. Inhalts- und Indexdaten von Nachrichten (mit der Ausnahme von Feldern wie Datum und anderen nicht personenbezogenen Informationen) werden unter Anwendung von auf Industriestandards beruhenden Verschlüsselungstechniken und auf der Basis eines kundenspezifischen, nur von dem betreffenden Kunden verwendbaren Verschlüsselungscode verschlüsselt. Nur der Kunde hat Zugriff auf alle Kennwörter, Verschlüsselungscodes und Konfigurationseinstellungen und sollte daher sicherstellen, dass diese sicher verwahrt und bei einem Treuhänder hinterlegt oder an einem anderen geeigneten Ort aufbewahrt werden.

B.11.4. Aufbewahrungsrichtlinien. Der Kunde kann Aufbewahrungsrichtlinien über die Benutzeroberfläche definieren und aktualisieren. In jeder Aufbewahrungsrichtlinie können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Phrasen im Inhalt sowie die Typen angehängter Dateien. Bei Archivierung einer Nachricht wird diese anhand der jeweils aktiven Aufbewahrungsrichtlinien bewertet. Falls eine Nachricht mehr als einer Aufbewahrungsrichtlinie entspricht, wird die Richtlinie mit der längsten Aufbewahrungszeit angewendet. Wenn die Nachricht keiner bestimmte Aufbewahrungsrichtlinie entspricht, wird die Standardaufbewahrungsrichtlinie angewendet.

B.11.5. InfoTags (Metadaten). Der Kunde kann InfoTags über die Benutzeroberfläche definieren und aktualisieren. In jedem InfoTag können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Phrasen im Inhalt sowie die Typen angehängter Dateien. Bei Archivierung einer Nachricht wird diese mit der jeweils aktiven Gruppe von InfoTags verglichen und mit dem zutreffenden InfoTag gekennzeichnet.

B.11.6. Richtlinienvorfahrung. An Aufbewahrungs- und Überwachungsrichtlinien vorgenommene Änderungen werden vom System in einer nicht änderbaren Form zur späteren Bezugnahme geführt. Der Kunde kann von aktuellen oder früheren Richtlinienversionen über die Benutzeroberfläche Dateien im PDF-Format erstellen.

B.11.7. Verfahrung archivierter Benutzer. Dem System wird jede Nacht eine Liste aller Benutzern mit einem Exchange-Postfach übergeben, damit eine fortlaufende Liste aller seit der Implementierung des Archiving.cloud (P) Service bestehenden Postfächer geführt wird.

B.11.8. Stubbing von Anhängen. Der Kunde kann Funktionen aktivieren, die die Inhalte von Anhängen im E-Mail-System des Kunden ("Postfachdaten") durch einen Hinweis auf die entsprechende Kopie im Archiv ersetzen. Der Kunde kann Stubbing-Richtlinien mit verschiedenen Regeln für jede Postfachgruppe basierend auf dem Alter und der Größe der Nachricht sowie des Ordners, in dem sie abgelegt ist, definieren und aktualisieren. Um die automatische Wiederherstellung des ursprünglichen Anhangs aus dem Archiv zu ermöglichen, wenn Benutzer E-Mails weiterleiten, kann der Kunde das benutzerdefinierte Formular zum Stubbing von Anhängen in der Organisationsformularbibliothek (einem speziellen öffentlichen Ordner auf dem Exchange-Server) installieren. Microsoft Outlook® installiert anschließend automatisch das benutzerdefinierte Formular vom Server. Um den Zugriff zum Abrufen von Anhängen außerhalb des Netzwerks des Kunden zu ermöglichen, kann der Kunde den Archiv-Proxy auf den Front-End (OWA) Exchange-Servern installieren. In der Standardeinstellung werden nur bereits archivierte Postfachdaten einem Stubbing-Verfahren unterzogen. Der Kunde kann eine Option aktivieren, mit der eine Kopie von Anhängen gespeichert wird, die nicht zuvor archiviert wurden, um zu ermöglichen, dass im Postfach enthaltene Anhänge einem Stubbing-Verfahren unterzogen werden. Der Kunde kann Aufbewahrungsrichtlinien pro Postfach konfigurieren, um zu definieren, wie lange Anhänge auf diese Weise aufbewahrt werden sollen. Falls keine solche Festlegung erfolgt ist, wird die Standardaufbewahrungsrichtlinie auf diese Elemente angewendet. Mittels dieses Vorgangs gespeicherte Anhänge können im Archiv nicht durchsucht werden.

B.11.9. Endbenutzerzugriff. Der Kunde kann einzelnen Benutzern Zugriffsmöglichkeiten zum Zweck der Durchsuchung des Archivs entweder innerhalb der Webbenutzeroberfläche oder direkt in Microsoft Outlook® bereitstellen.

B.11.10. Zugriff für Beweissicherung. Der Kunde kann innerhalb der Benutzeroberfläche Suchvorgänge im gesamten Archiv durchführen. Der Kunde kann einen Aufbewahrungsort für den Vernichtungsstopp aus juristischen Überlegungen ("Legal Hold") einrichten. Dabei handelt es sich um ein Repository für Nachrichten, die für eine bestimmte Angelegenheit relevant sind. Der Kunde kann dieses Repository genauso durchsuchen wie das aktive Archiv.

B.11.11. Ad-Hoc-Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen ("Ad-Hoc Legal Holds"). Der Kunde kann die Richtlinienbenutzeroberfläche nutzen, um Ad-hoc-Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen ("Ad-Hoc Legal Holds") zu definieren und aktualisieren. Für jeden "Legal Hold" können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Phrasen im Inhalt sowie die Typen angehängter Dateien. Bei Archivierung einer Nachricht wird diese anhand der jeweils aktiven "Legal Holds" bewertet. Die Nachricht wird mit jedem "Legal Hold" verknüpft, mit dem sie übereinstimmt. Um vorhandene archivierte Daten in einem "Ad-Hoc Legal Hold" zu erfassen, kann der Kunde eine Suche mit ähnlichen Kriterien durchführen, die Ergebnisse in einen Ordner kopieren und die Inhalte des Ordners anschließend in den "Legal Hold" kopieren. Die Aufbewahrungszeit für jeden "Ad-Hoc Legal Hold" ist unbegrenzt lang. Alle Nachrichten in einem bestimmten "Ad-Hoc Legal Hold" werden aufbewahrt, bis der betreffende "Ad-Hoc Legal Hold" freigegeben wird.

B.11.12. Personenbasierte Aufbewahrungsorte für den Vernichtungsstopp. Der Kunde kann die Richtlinienbenutzeroberfläche nutzen, um personenbasierte Aufbewahrungsorte zu definieren und zu aktualisieren. Jeder personenbasierte Aufbewahrungsort definiert eine Menge von Benutzern. Sofern eine Nachricht eine der an einem bestimmten Aufbewahrungsort aufgelisteten Personen betrifft, wird die Archivierung mit diesem Aufbewahrungsort verknüpft. Das System erfasst automatisch auch vorhandene, zu den Benutzern gehörende und momentan vom Aufbewahrungsort referenzierte E-Mails und erstellt eine neue Kopie der Nachrichten an dem Aufbewahrungsort. Wenn Benutzer aus der Definition eines personenbezogenen Aufbewahrungsorts entfernt werden, werden Nachrichten, die nur zu diesen Benutzern gehören, automatisch von diesem Aufbewahrungsort entfernt. Nachrichten für aktuell aufgelistete Benutzer, die von einem Aufbewahrungsort erfasst sind, werden aufbewahrt, bis der betreffende Aufbewahrungsort freigegeben wird.

B.11.13. Datenexport. Nachrichten können aus dem aktiven Archiv oder vom Aufbewahrungsort für den Vernichtungsstopp in PST-Dateien exportiert werden. Das System erstellt mehrere PST-Dateien, sollte dies aufgrund von Beschränkungen hinsichtlich der Dateigröße erforderlich werden.

B.11.14. Berichterstattung. Berichte zu Größe und Wachstum des Archivs stehen dem Kunden innerhalb der Benutzeroberfläche zur Verfügung und können im HTML-Format angezeigt oder in eine PDF- oder CSV-Datei (nur Daten) exportiert werden.

B.11.15. Audit-Pfad. Such-, Nachrichtenanzeige-, Export-, Abruf- und Überwachungsaktivitäten werden verfolgt. Der Audit-Pfad kann als Eigenschaft einer jeweiligen Nachricht angesehen werden. Ein Audit-Pfad-Viewer für alle Nachrichten ermöglicht gefilterte Ansichten abhängig von der Art der Aktivität, der Person, welche die Aktivität durchgeführt hat, und/oder dem Datum der Aktivität.

B.11.16. Integration mit Active Directory. Der Zugriff auf das Archiv wird verwaltet, indem Benutzer (oder vorhandene Benutzergruppen) einem Satz vordefinierter Sicherheitsgruppen in Active Directory hinzugefügt werden. Jeder dieser Gruppen ist ein Satz von Berechtigungen zugeordnet. Benutzer können aufgrund ihrer Mitgliedschaft in mehreren dieser Sicherheitsgruppen verschiedene Rollen ausüben. Die Authentifizierung erfolgt direkt anhand von Active Directory. Benutzer melden sich mit ihrem normalen Benutzernamen und Kennwort für Active Directory an. Deaktivierte Konten haben keinen Zugriff auf das Archiv. Active Directory-Gruppen können zum Zweck einer vereinfachten Verwaltung von Elementen wie Richtlinien auch über verschiedene andere Aspekte des Systems referenziert werden. Gruppenmitgliedschaftsänderungen werden mittels eines Synchronisierungsprozesses erfasst, der über Nacht durchgeführt wird.

B.11.17. Aufbewahrungs- und Entsorgungsverwaltung. Ausgehend von den vom Kunden innerhalb der SMC definierten Aufbewahrungsrichtlinien kategorisiert der Archiving.cloud (P) Service Nachrichten und weist ihnen entweder ein geplantes Entsorgungsdatum zu oder zeichnet im Fall einer unbefristeten Aufbewahrung den Monat auf, in dem die Nachricht archiviert wurde. Die geplanten Entsorgungstermine fallen jeweils auf den Monatsbeginn. Sobald Nachrichten das für sie vorgegebene Entsorgungsdatum erreicht haben, kann bzw. können der bzw. die berechnigte(n) Benutzer des Kunden die Entsorgung für alle Nachrichten formal bewilligen, die diesem geplanten Entsorgungsdatum zugeordnet sind. Bei Nachrichten, die mit Blick auf eine unbegrenzt lange Aufbewahrungszeit archiviert wurden, kann bzw. können der bzw. die berechnigte(n) Benutzer des Kunden die Entsorgung für alle Nachrichten formal bewilligen, die in einem bestimmten Monat archiviert wurden. Für eine Entsorgung vorgesehene Daten können aus Speichermedien jeglicher Art (einschließlich und ohne Beschränkung aus Backup-Kopien) nicht so wiederhergestellt werden, dass sie visuell lesbar sind.

B.12. **Premium-Funktionen**

Folgende Funktionen stehen nur beim Symantec Email Archiving.cloud Premium (P) Service zur Verfügung:

B.12.1. Überwachung:

- a) Automatische Auswahl für aufsichtliche Überprüfung. Der Kunde kann Richtlinien definieren und aktualisieren, die Nachrichten zu einer Überprüfungswarteschlange hinzufügen. In jeder Richtlinie können die beteiligten Parteien, Schlüsselwörter/Phrasen im Inhalt und Dateitypen berücksichtigt werden. Ferner können Stichprobenrichtlinien für bestimmte Benutzer konfiguriert werden.
- b) Aufsichtliche Überprüfung. Der Kunde kann Zugriffsrechte für Prüfer zuweisen, um Nachrichten zu lesen, die der Überprüfungswarteschlange hinzugefügt wurden, und diese als zulässig oder nicht zu kennzeichnen.

B.12.2. Bloomberg®-Archivierung:

- a) Der Symantec Email Archiving.cloud Premium (P) Service nutzt Protokollfunktionen des Bloomberg® Professional Service, der E-Mail-Nachrichten und Instant Messaging-Gespräche in XML-Dateien aufzeichnet, die jede Nacht auf die FTP-Site von Bloomberg® übertragen werden.
- b) Wenn der Kunde den Bloomberg® Professional Service abonniert, kann die E-Mail-Archivierungs-Appliance genutzt werden, um eine Kopie dieser XML-Dateien von der FTP-Site zur Umwandlung in Nachrichten im HTML-Format und zur Versendung an das Archiv abzurufen.
- c) Das FIRM-Format wird unterstützt, nicht jedoch das ACCOUNT-Format oder das ursprüngliche Extraktionsformat von Bloomberg®-Protokollen.
- d) Im Zuge der Bloomberg®-Archivierungsintegration wird kein Inhalt auf der FTP-Site von Bloomberg® gelöscht. Es wird dabei jedoch aufgezeichnet, welche Dateien verarbeitet wurden. Da über Bloomberg® regelmäßig Inhalte von der FTP-Site entfernt und beim Bloomberg-Archivierungsintegrationsprozess Kopien gelöscht werden, die von Bloomberg® in den E-Mail-Archivierungseinrichtungen erstellt wurden, muss der Kunde überwachen, ob die Archivierungsintegration ständig betrieben werden kann, so dass Dateien, bevor sie mithilfe der Bloomberg®-Archivierungsintegration abgerufen und vollständig verarbeitet werden können, nicht gelöscht werden.
- e) Um zu identifizieren, welche in der Extensible Markup Language (XML) referenzierten Benutzer interne Mitarbeiter sind, wird eine Liste mit Bloomberg®-FIRM-IDs verwendet. Die Bloomberg®-Archivierungsintegration stellt eine webbasierte Zuordnungsbenutzeroberfläche bereit, die ermöglicht, dass ein Administrator die Bloomberg®-Benutzerkonten jeweils den entsprechenden Active Directory-Benutzerkonten zuordnet. Wenn die XML-Dateien verarbeitet werden und eine Nachricht einen internen Benutzer referenziert, der noch nicht zugeordnet wurde, wird die Adresse der nicht zugeordneten Adressliste hinzugefügt und die Nachricht wird nicht verarbeitet. Sobald der Administrator diese Adressen zugeordnet hat, können sie die erneute Verarbeitung der verknüpften Nachrichten auslösen. Die aufgelösten E-Mail-Unternehmensadressen werden als Adressen der Absender/Empfänger der Nachricht verwendet.
- f) Ein Informationsblock im Nachrichtentext liefert zusätzliche Informationen zu den tatsächlichen Adressen/Anzeigenamen der Nachrichten-/Gesprächsparteien, einschließlich der Bloomberg®-Kontoinformationen des betreffenden Benutzers.

B.13. **Altdateienimport**

B.13.1. Vorbehaltlich der Entrichtung einer Gebühr basierend auf der Menge der zu importierenden Daten kann der Kunde Altdateien in den Archiving.cloud (P) Service importieren. Für den Fall, dass die tatsächliche Menge der Altdateien die Menge der erworbenen Importdaten übersteigt, behält Symantec sich das Recht vor, die für diese zusätzlichen Daten entstehenden Kosten zu den jeweiligen Standardpreisen in Rechnung zu stellen.

B.13.2. Entscheidet sich der Kunde, zur Erleichterung des Datenimports unabhängige Software von Dritten zu nutzen, akzeptiert der Kunde, dass dies auf eigenes Risiko und eigene Kosten erfolgt.

C. **Pflichten des Kunden**

C.1. Der Kunde muss eine oder mehrere E-Mail-Archivierungs-Appliances erwerben, um den Archiving.cloud (P) Service nutzen zu können. Die E-Mail-Archivierungs-Appliance(s) (und Begleitdokumentation) werden zur Installation und Konfiguration an den Kunden geliefert. Der Kunde ist für sämtliche Frachtkosten, Einfuhrzölle, Versicherungsprämien und Steuern für die E-Mail-Archivierungs-Appliance verantwortlich.

C.2. Alle in der Setup-Anleitung (Client Setup Document) Dokument von Symantec beschriebenen Aktionen müssen vom Kunden vor der anfänglichen Telekonferenz durchgeführt worden sein. Dazu gehören unter anderem:

- a) Einrichten neuer Active Directory-Benutzerkonten
- b) Einrichten zusätzlicher Active Directory-Gruppen
- c) Hinzufügen von Benutzern zu Exchange-Gruppen
- d) Firewall-Konfiguration (falls erforderlich)

- e) Aktivieren von Microsoft Exchange® Journaling (frühestens 48 Stunden vor Installation der E-Mail-Archivierungs-Appliance)
- f) Installieren der E-Mail-Archivierungs-Appliance (im Rack und hochgefahren)
- g) Sicherstellen, dass alle zur Archivierung erforderlichen Postfächer "E-Mail-aktiviert" sind
- h) Konfigurieren des Remote-Zugriffs für Symantec

C.3. Der Kunde kann sich an einen Symantec Customer Service Manager wenden, falls bei den oben genannten Aktionen Hilfe benötigt wird.

C.4. Der Kunde muss die Journaling-Funktion von Exchange konfigurieren, um eine Kopie interner und externer E-Mails in einem lokalen Postfach auf dem Exchange-Server abzulegen. Anschließend können Appliances, die sich im Unternehmensnetzwerk des Kunden hinter der Firewall befinden ("E-Mail-Archivierungs-Appliances") eingesetzt werden, um aus diesem Postfach Daten zur Übergabe an den Archiving.cloud (P) Service abzurufen. E-Mails werden erst im Journaling-Postfach gelöscht, wenn die Speicherung im Archiving.cloud (P) Service bestätigt wurde.

D. Berichterstattung. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Archivierte E-Mails können erst nach Ablauf des zugewiesenen Aufbewahrungszeitraums gelöscht werden.

F.2. Symantec kann nicht als Drittanbieter für Downloads fungieren. Für den Fall, dass der Kunde aus Compliance-Gründen einen Drittanbieter für Downloads bestimmen muss, muss der Kunde einen unabhängigen Vertrag mit dem externen Serviceanbieter von Symantec eingehen. Dafür kann eine separate Gebühr anfallen, die nicht von Symantec festgesetzt wird.

F.3. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

F.4. Bei Kündigung des Archiving.cloud (P) Service löscht Symantec die Daten des Kunden aus dem Archiv. Vor der Kündigung kann der Kunde seine Daten aus dem Archiv extrahieren, oder der Kunde kann anfordern, dass der von Symantec autorisierte Drittanbieter die archivierten Daten im PST-Dateiformat zurück an den Kunden überträgt.

F.5. Falls der Kunde bei Kündigung eine Übertragung der archivierten Daten durch den von Symantec autorisierten Drittanbieter anfordert, gilt Folgendes:

- a) Der Kunde muss eine direkte Vereinbarung mit diesem Drittanbieter abschließen. Symantec ist kein Vertragspartner in einer solchen Vereinbarung.
- b) Da die Daten in einem verschlüsselten Format gespeichert werden, muss der Kunde dem Drittanbieter einen Verschlüsselungscode bereitstellen, um die E-Mails in ein unverschlüsseltes Format dekodieren zu können.
- c) Der Kunde trägt die Kosten der Übertragung. Die Kosten werden in der Vereinbarung mit dem Drittanbieter vereinbart. Die Höhe der Kosten hängt von folgenden Faktoren ab: (i) Datenmenge; (ii) Format/Medium der Übertragung; (iii) Kosten für die Einrichtung des Übertragungsprozesses; (iv) Zeit- und Materialaufwand für die Durchführung der Übertragung.
- d) Symantec behält sich das Recht vor, seine zu diesem Zeitpunkt geltenden Gebühren für die Speicherung in Rechnung zu stellen, falls die Daten zum Datum des Inkrafttretens der Kündigung nicht exportiert und gelöscht wurden.

F.6. Symantec ist berechtigt, den Archiving.cloud (P) Service nach alleinigem Ermessen ohne Vorankündigung umgehend zu kündigen und jegliche von Symantec als notwendig erachtete Abwehrmaßnahmen zu ergreifen:

- a) Im Fall einer Anweisung durch ein Gericht oder eine zuständige Behörde
- b) Im Fall eines Angriffs auf den Archiving.cloud (P) Service oder das Netzwerk
- c) Im Fall, dass der Kunde oder seine Benutzer gegen die unten definierte Nutzungsrichtlinie verstoßen.

F.7. Der Kunde hat sicherzustellen, dass er und alle seine Benutzer diese Nutzungsrichtlinie kennen und einhalten:

Die Benutzer dürfen unter keinen Umständen weder vorsätzlich, fahrlässig oder schuldlos Handlungen begehen bzw. versuchen oder Beihilfe leisten, die eine Bedrohung des Archiving.cloud (P) Service bewirken können. Zu solchen Handlungen zählen unter anderem:

- a) Jegliche Versuche, einen Service-Host oder ein Netzwerk zum Absturz zu bringen
- b) "Denial-of-Service"-Angriffe oder "Flooding"-Angriffe auf einen Service-Host oder ein Netzwerk

- c) Jegliche Versuche, die Benutzerauthentifizierung oder Sicherheit eines Service-Hosts oder Netzwerks zu umgehen
- d) Die Erstellung, Übermittlung, Speicherung oder Veröffentlichung von Viren, schädigenden Programmen oder beschädigten Daten jeglicher Art
- e) Jegliche sonstige Handlungen, die sich nachteilig auf den Archiving.cloud (P) Service oder dessen Betrieb auswirken können

F.8. SYMANTEC ÜBERNIMMT KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT AUF SERVICEAUSFÄLLE ZURÜCKZUFÜHREN SIND. DAVON UNBERÜHRT BLEIBEN DIE RECHTSMITTEL, DIE IM SERVICE LEVEL AGREEMENT (SLA) AUSDRÜCKLICH VORGESEHEN SIND.

F.9. Symantec haftet nicht für den Verlust von Kennwörtern, Verschlüsselungscodes oder Konfigurationseinstellungen. Der Kunde akzeptiert und stimmt zu, dass der Verlust von Kennwörtern und Verschlüsselungscodes zur Folge hat, dass kein Zugriff auf das Archiv möglich ist.

F.10. Der Kunde muss den Ort des Archivierungsrechenzentrums bei der Bestellung auswählen, und die Gebühren werden basierend auf dieser Auswahl berechnet. DER KUNDE VERPFLICHTET SICH, ALLE NOTWENDIGEN MASSNAHMEN ZU ERGREIFEN, UM (I) SEINE MITARBEITER, VERTRETER UND AUFTRAGNEHMER SOWIE DRITTE, DIE DAS ZUM ARCHIVING.CLOUD (P) SERVICE GEHÖRENDE KOMMUNIKATIONSSYSTEM NUTZEN, DARÜBER ZU INFORMIEREN, DASS JEGLICHE INFORMATIONEN, INSBESONDERE PERSONENBEZOGENE INFORMATIONEN ZU EINZELNEN PERSONEN, AM STANDORT DES RECHENZENTRUMS VERARBEITET WERDEN KÖNNEN, UND SOLLTE DIES GESETZLICH VORGESCHRIEBEN SEIN, (II) DIE ZUSTIMMUNG DIESER MITARBEITER, VERTRETER, AUFTRAGNEHMER UND DRITTEN ZU EINER SOLCHEN VERARBEITUNG EINZUHOLEN, BEVOR DER KUNDE DEN ARCHIVING.CLOUD (P) SERVICE AUSFÜHRT.

F.11. Der Kunde erkennt an und stimmt zu, dass, falls erworben, (i) die Scan-Services von Symantec (Email AntiVirus.cloud, Email AntiSpam.cloud, Email Image Control.cloud und Email Data Protection.cloud) nicht alle E-Mails scannen, die ursprünglich im Archiv eingehen, und (ii) die Scan-Services von Symantec (Email AntiVirus.cloud, Email AntiSpam.cloud, Email Image Control.cloud und Email Data Protection.cloud) keine E-Mails scannen, die aus dem Archiv für eine Wiederherstellung in den Benutzerpostfächern freigegeben werden. Dementsprechend übernimmt Symantec keine Haftung für Viren, Spam, Bilder oder unangemessene Inhalte, die in solchen wiederhergestellten E-Mails enthalten sein können. Darüber hinaus finden das Service Level Agreement auf diese wiederhergestellten E-Mails keine Anwendung.

Anhang 18 – Symantec Web Security Archiving.cloud

A. Serviceübersicht

A.1. Der Symantec Web Security Archiving.cloud Service ist ein Cloud-basierter Archivierungsservice, der zur Aufbewahrung des Browserverlaufs der Benutzer aus den Symantec Web Services dient.

B. Servicemerkmale

B.1. Der Kunde hat die Wahl zwischen Basic Service und Premium Service:

B.1.1. Der Basic Service umfasst Folgendes:

- a) Einen Standardzeitraum von 6 Monaten
- b) Ermöglicht bis zu 12 Monate Archivierung

B.1.2. Der Premium Service umfasst Folgendes:

- a) Einen Standardzeitraum von 3 Jahren
- b) Ermöglicht bis zu 7 Jahre Archivierung
- c) Eine SMC, über die jeder Benutzer direkt auf die Elemente in seinem eigenen Archiv zugreifen kann. Benutzer können ihr gesamtes Archiv durchsuchen, haben jedoch keinen Zugriff auf die erweiterten Funktionen, die dem Archivadministrator zur Verfügung stehen. Benutzer haben keinen Zugriff auf Informationen im Archiv, die nicht von ihnen selbst erstellt wurden.

B.2. Der Service ermöglicht die Archivierung der folgenden Informationen:

- a) Datum, an dem die URL angefordert wurde
- b) Benutzer, der die URL angefordert hat
- c) Vollständige angeforderte URL
- d) RuleSpace-Kategorie gemäß Definition durch Web Security Service

B.3. Die Informationen werden ausschließlich aus den von den Web Services erzeugten Protokollen generiert und werden innerhalb der Symantec-Infrastruktur aufgenommen, indexiert und gespeichert. Es werden alle URLs gespeichert, ausgenommen solcher, die der Umgehungsliste (Bypass List) in den Symantec Web Services hinzugefügt wurden.

B.4. Die E-Discovery-Funktion ermöglicht das Durchsuchen von Daten mithilfe mehrerer Suchfelder und Optionen.

B.5. Es sind Datenvernichtungsstopps verfügbar, damit Protokolle gruppiert, benannt und gespeichert werden können. Die Daten werden dann für einen unbegrenzten Zeitraum aufbewahrt, entweder bis der Vernichtungsstopp aufgehoben wird oder bis der Service vom Kunden gekündigt wird.

B.6. Datensätze können zur externen Prüfung und/oder Speicherung in das HTML-Format exportiert werden.

B.7. Es werden Verschlüsselungstechnologien eingesetzt, um sicherzustellen, dass sämtliche Kommunikation zwischen Service und Archiv verschlüsselt ist. Die Daten sind auch bei der Speicherung innerhalb des Archivs vollständig verschlüsselt und können außer vom Kunden von niemandem unverschlüsselt abgerufen werden.

C. Pflichten des Kunden

C.1. Der Kunde ist dafür zuständig, den Protokollaufbewahrungszeitraum in der SMC zu konfigurieren.

C.2. Der Kunde muss die erforderlichen Informationen für alle autorisierten Benutzer des Service hochladen.

D. Berichterstattung.

D.1. Dem Serviceadministrator stehen die folgenden Berichtsmetriken zur Verfügung: Anzahl Benutzer, insgesamt genutzter Speicherplatz sowie pro Tag genutzter Speicherplatz.

E. Technischer Support. Siehe Anlage 1, Definitionen und allgemeine Serviceübersicht.

F. Zusätzliche Bestimmungen und Bedingungen.

F.1. Archivierte Webdatensätze können erst aus dem System gelöscht werden, wenn der vom Kunden bestimmte Aufbewahrungszeitraum abgelaufen ist.

F.2. Der Kunde erkennt an, dass Symantec keine Daten abrufen kann, die vom Service verschlüsselt wurden.

F.3. Das Service Level Agreement (SLA) in Anlage 3 unten ist nicht für den Basic Service wirksam.

F.4. SYMANTEC ÜBERNIMMT KEINE HAFTUNG FÜR DIE BESCHÄDIGUNG ODER DEN VERLUST VON DATEN, DIE SICH DIREKT ODER INDIREKT AUS EINER NICHT ERFOLGTEN ARCHIVIERUNG VON DATEN DURCH DEN SERVICE ERGEBEN.

Anhang 19 – Symantec Endpoint Protection Small Business Edition 2013

A. Serviceübersicht

A.1. Der Symantec Endpoint Protection Small Business Edition 2013 Service ist ein Antivirus- und Anti-Malware-Service, bei dem der Kunde zwischen einem Cloud-verwalteten Service oder einer Vor-Ort-Bereitstellungsoption wählen kann. Dieser Anhang gilt lediglich für die Cloud-verwaltete Bereitstellungsoption. Die Vor-Ort-Option unterliegt dem Abonnementinstrument und der zugehörigen Endbenutzer-Lizenzvereinbarung (EULA).

B. Servicemerkmale

B.1. Der Service hat folgende Aufgaben:

- a) Schützen des Computers vor erkannter Malware auf der Grundlage bekannter Methoden.
- b) Blockieren bekannter bösartiger Angriffe, die aus dem Netzwerk auf den Computer erfolgen.
- c) Bereitstellen verfügbarer Antiphishing-Funktionalität in unterstützten Browsern, die vermutete Phishing-Angriffe blockieren soll.
- d) Symantec veröffentlicht die aktuelle Liste unterstützter Computerbetriebssysteme für den Agenten sowie unterstützter Browser für die SMC.
- e) Blockieren oder Zulassen des Zugriffs von USB-Speichergeräten gemäß kundenspezifischer Konfiguration.

B.2. An den Richtlinien vorgenommene Änderungen sind in der SMC sichtbar und werden im Stapelmodus an die Agenten verteilt. Die jeweils wirksamen Richtlinieneinstellungen für einzelne Agenten können in der SMC oder in dem auf dem Endbenutzercomputer ausgeführten Agenten angezeigt werden.

B.3. Der Kunde kann den Service so konfigurieren, dass eine automatische Benachrichtigung an konfigurierte E-Mail-Empfänger gesendet wird. Die Benachrichtigungen basieren auf der Regel für Warnmeldungen, die in der SMC konfiguriert werden kann. Benachrichtigungen können über die SMC erstellt, gelöscht und angepasst werden.

C. Pflichten des Kunden

C.1. Die Servicesoftware muss auf jedem Endbenutzercomputer installiert werden, der den Service empfängt.

C.2. Der Kunde muss die Servicesoftware über die SMC verwalten.

C.3. Der Kunde muss Computer, Richtlinien, Warnmeldungen, Berichte und andere Konfigurationsoptionen über die SMC verwalten.

C.4. Der Kunde muss erforderliche Firewall-Änderungen vornehmen, damit der Agent mit dem Service kommunizieren und zusammenarbeiten kann.

C.5. Der Kunde muss lokale Update-Hosts über die SMC festlegen.

D. Berichterstattung

D.1. Während der Laufzeit des Service werden sämtliche vom Agenten erstellten Protokolle und Berichte für einen Zeitraum von neunzig (90) Tagen in der SMC gespeichert und können während dieses Zeitraums darüber angezeigt und von dort heruntergeladen werden. Nach Ablauf dieser 90-tägigen Frist werden die Protokolle und Berichte automatisch gelöscht.

D.2. Sämtliche Protokolle und Berichte werden nach Kündigung oder Laufzeitende des Service gelöscht.

E. Technischer Support

E.1. Zu den Supportleistungen gehören:

- a) Führung durch die SMC, einschließlich einer Servicebeschreibung sowie einer Frage- und Antwortsitzung (Dies schließt keine Hilfestellung bei der Einrichtung von Richtlinien oder der Analyse der Richtlinienwirksamkeit ein.)
- b) Onlinehilfe-Inhalte
- c) Benutzerhandbuch

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Instanzen: Ungeachtet jeglicher widersprüchlicher Aussagen in diesem Anhang muss jede laufende Instanz der Servicesoftware (ob physisch oder virtuell) entsprechend lizenziert sein. Eine "Instanz" der Servicesoftware wird durch Ausführen des Setup- oder Installationsverfahrens der Servicesoftware erstellt. Eine "Instanz" der Servicesoftware wird durch Duplizieren einer vorhandenen Instanz erstellt. Verweise auf die Servicesoftware beinhalten "Instanzen" der Servicesoftware. Das "Ausführen einer Instanz" der Software durch den Kunden erfolgt, indem dieser die Software in

den Arbeitsspeicher lädt und mindestens eine der darin enthaltenen Anweisungen ausführt. Wird eine Instanz ausgeführt, gilt sie so lange als ausgeführt (unabhängig davon, ob ihre Anweisungen weiterhin ausgeführt werden oder nicht) bis sie aus dem Speicher entfernt wird.

F.2. Terminalserver: Wenn die Servicesoftware zur Nutzung auf einem Hardwaregerät/Server bestimmt ist, das/der Endgeräte mit einem gemeinsamen Verbindungspunkt zu einem lokalen oder Weitverkehrsnetzwerk bereitstellt ("lizenzierter Terminalserver"), und auf derartige lizenzierte Terminalserver von Endgeräten zugegriffen wird, auf denen keine Kopie der Servicesoftware installiert ist ("Thin Clients"), wird jeder Thin Client, der auf einen lizenzierten Terminalserver zugreift, als "Instanz" betrachtet und muss über eine gültige Lizenz für die Servicesoftware verfügen. Falls auf den oder die lizenzierten Terminalserver Endgeräte zugreifen, auf denen bereits autorisierte Kopien der Servicesoftware installiert sind ("Thick Clients"), werden solche Zugriffe auf lizenzierte Terminalserver durch Thick Clients nicht als zusätzliche Instanzen angesehen, und der Kunde muss keine zusätzlichen Lizenzen für die Servicesoftware erwerben.

F.3. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

F.4. Wie im geltenden Abonnementinstrument angegeben, kann der Kunde entscheiden, während der geltenden Lizenzlaufzeit zu einem beliebigen Zeitpunkt entweder die Cloud-verwaltete Option oder die Vor-Ort-Option bereitzustellen, jedoch nicht beide zur gleichen Zeit. Unabhängig davon, wann der Service erworben wurde, müssen alle Benutzer des Service dieselbe Bereitstellungsoption nutzen. Wenn der Kunde von einer Bereitstellungsoption zur anderen wechselt, wird ihm eine Kulanzfrist von sechzig (60) Kalendertagen gewährt, um diese Umstellung vorzunehmen. Wenn sich der Kunde für die Bereitstellung der Vor-Ort-Option entscheidet, muss er innerhalb von neunzig (90) Tagen nach Verfügbarkeit des entsprechenden Upgrades auf die aktuellste Version aktualisieren.

F.5. Bei Nutzung des Cloud-verwalteten Service ist der Kunde berechtigt, die Vor-Ort-Option zum Schutz einer Umgebung bereitzustellen, für die der Cloud-verwaltete Service noch nicht verfügbar ist. Jegliche Bereitstellung der Vor-Ort-Option muss in der Gesamtanzahl der Benutzer berücksichtigt werden. Sobald der Cloud-verwaltete Service für diese Umgebung verfügbar wird, stehen dem Kunden sechzig (60) Kalendertage zur Verfügung, um die Bereitstellung für alle Benutzer zu synchronisieren.

Anhang 20 – Symantec Backup Exec.cloud

A. Serviceübersicht

A.1. Der Symantec Backup Exec.cloud Service ermöglicht die Online-Sicherung und -Wiederherstellung von durch den Kunden ausgewählten Daten.

B. Servicemerkmale

B.1. Der Service leitet Kundendaten automatisch in Rechenzentren von Symantec weiter.

B.2. Der Kunde kann den Service über die SMC so konfigurieren, dass Kundendaten direkt auf unternehmensinterne Speicherorte ("Onsite Backup") gesichert werden. Onsite Backup kann nur von Benutzern genutzt werden, die direkt (physisch oder virtuell) mit der Umgebung des Kunden verbunden sind. Die Speicherkapazität für Onsite Backup hängt von dem in der Kundenumgebung verfügbaren Speicher ab. Onsite Backup kann Daten automatisch mit den Rechenzentren von Symantec synchronisieren, wenn diese Option vom Kunden konfiguriert wird.

B.3. Die Daten sind während der Übertragung und im Speicher verschlüsselt.

B.4. Symantec verpflichtet sich, eine Liste der unterstützten Computerbetriebssysteme für die Nutzung und Installation des Agenten sowie der unterstützten Browser zur Nutzung der SMC zu veröffentlichen. Der Kunde erkennt an und stimmt zu, dass Symantec diese Liste regelmäßig und ohne vorherige Ankündigung aktualisieren und ändern kann.

B.5. Die auf dem betreffenden Benutzercomputer installierte Servicesoftware sichert die Daten in Symantec-Rechenzentren und/oder unternehmensintern per Onsite Backup. Welche Daten gesichert werden, richtet sich danach, welche Dateien/Ordner über die SMC ausgewählt wurden.

B.6. Vom Kunden gewählte Änderungen, die über die SMC vorgenommen wurden, sind auf der SMC umgehend sichtbar. Die Endbenutzerkonfigurationen werden anschließend im Stapelmodus an die Servicesoftware verteilt, sobald die Endgeräte online und verfügbar sind.

B.7. Der Kunde kann den Service so konfigurieren, dass eine automatische Benachrichtigung an konfigurierte E-Mail-Empfänger gesendet wird. Die Benachrichtigungen basieren auf vordefinierten Warnmeldungen, die der Kunde in der SMC konfigurieren kann.

B.8. Der Kunde kann Benachrichtigungen über die SMC erstellen, löschen und anpassen.

C. Pflichten des Kunden

C.1. Der Kunde muss die Servicesoftware auf den jeweiligen Benutzercomputern installieren und über die SMC entsprechende Richtlinien zur Nutzung des Service zuweisen.

C.2. Der Kunde muss ggf. einige grundlegende Firewall-Änderungen vornehmen, damit die Servicesoftware mit der Service-Infrastruktur kommunizieren und zusammenarbeiten kann.

C.3. Der Kunde muss die SMC zur Verwaltung der Servicesoftware verwenden.

D. Berichterstattung

D.1. Sämtliche vom Agenten erstellten Protokolle und Berichte werden für einen Zeitraum von neunzig (90) Tagen in der SMC gespeichert und können während dieses Zeitraums darüber angezeigt und von dort heruntergeladen werden. Nach Ablauf dieser Frist werden die Protokolle und Berichte gelöscht.

E. Technischer Support

E.1. Zu den Supportleistungen gehören:

- a) Führung durch die SMC per Telekonferenz, einschließlich einer Servicebeschreibung sowie einer Frage- und Antwortsitzung. (Dies schließt keine Hilfestellung bei der Einrichtung von Richtlinien oder der Analyse der Richtlinienwirksamkeit ein.)
- b) Zugriff auf das Administratorhandbuch und das Benutzerhandbuch, die beide über die SMC abgerufen werden können.

F. Zusätzliche Bestimmungen und Bedingungen

F.1. Sämtliche von Symantec oder deren Drittanbietern im Rahmen dieser Vereinbarung gespeicherten oder archivierten Kundendaten sind alleiniges Eigentum des Kunden ("Kundendaten"). Keine der in diesem Anhang enthaltenen Bestimmungen überträgt Symantec oder deren Anbietern irgendwelche gesetzlichen oder billigskeitsrechtlichen Rechte, Titel oder Interessensansprüche an den Kundendaten.

F.2. Der Kunde übernimmt die alleinige Verantwortung für das Verhalten des Kunden hinsichtlich des Service, einschließlich Kontrolle über den Inhalt der auf dem Service gespeicherten Kundendaten. Der Kunde verpflichtet sich insbesondere, bei Verwendung des Service Folgendes zu unterlassen:

- a) Gegen geltende Gesetze und Regeln zu verstoßen, einschließlich, aber nicht beschränkt auf das Hochladen, Übertragen, Speichern oder anderweitige Sichern obszöner, sittenwidriger oder pornografischer Inhalte
- b) Den Service auf irgendeine Art zu verwenden, die gegen Rechte an geistigem Eigentum oder gegen andere Rechte Dritter verstößt, oder
- c) Material zu übertragen, das Viren oder anderen schädigenden Computercode oder Dateien wie Trojaner, Würmer oder Zeitbomben enthält

F.3. Der Kunde kann so lange Kundendaten hochladen, speichern oder anderweitig sichern, bis die Gesamtmenge an Speicher bzw. das zugeteilte Speicherkontingent, das der Kunde von Symantec erworben hat ("maximale Speichermenge"), erreicht ist. Für den Fall, dass der Kunde die maximale Speichermenge überschreitet, behält sich Symantec das Recht vor, die Datensicherungsrechte des Kunden so lange einzuschränken, bis dieser seinen Speicherbedarf reduziert oder einen Speicherplan mit höheren Kontingenten abonniert.

F.4. Der Kunden kann während der Servicelaufzeit innerhalb einer Frist von neunzig (90) Tagen auf Kundendaten zugreifen. Nach Ablauf oder Kündigung der Servicelaufzeit sind die Kundendaten für den Kunden nicht mehr verfügbar. Dem Kunden ist es nicht gestattet, weitere Sicherungskopien hinzuzufügen oder Kundendaten wiederherzustellen. Symantec verpflichtet sich jedoch, die Kundendaten ("gespeicherte Daten") für einen Zeitraum von sechzig (60) Kalendertagen nach Laufzeitende oder Kündigung des Service ("Aufbewahrungszeitraum nach Ablauf") zu speichern und zu verwalten. Während des "Aufbewahrungszeitraums nach Ablauf" kann der Kunde entscheiden, die Laufzeit zu verlängern und die anfallenden Gebühren zu entrichten, um so erneut Zugriff auf die zuvor gespeicherten Daten zu erhalten. Nach Verstreichen des "Aufbewahrungszeitraums nach Ablauf" werden die Kundendaten von Symantec gelöscht und der Zugriff auf die Daten für Symantec und für den Kunden gesperrt, sollte der Kunde den Service nicht verlängern.

F.5. Der Kunde kann mit Onsite Backup gesicherte Daten nur in der kundeneigenen und/oder vom Kunden kontrollierten Umgebung speichern. Mit Onsite Backup gesicherte Daten dürfen nicht an einen Managed Service Provider oder Servicebüroserver weitergeleitet werden.

F.6. DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN VEREINIGTEN STAATEN ERBRACHT WERDEN KÖNNEN.

ANLAGE 3 SERVICE LEVEL AGREEMENT (SLA)

1. Allgemein

1.1. Falls der Kunde der Ansicht ist, dass er Anspruch auf ein Rechtsmittel gemäß diesem Service Level Agreement hat, muss der Kunde innerhalb von zehn (10) Werktagen ab dem Ende des jeweiligen Kalendermonats, in dem der mutmaßliche Verstoß gegen den Service Level aufgetreten ist, einen Gutschriftenantrag einreichen. Der Kunde erkennt an, dass Protokolle nur für eine begrenzte Zahl von Tagen aufbewahrt werden und deshalb außerhalb des vorgegebenen zeitlichen Rahmens eingereichte Gutschriftenanträge als ungültig betrachtet werden.

1.2. Alle Gutschriftenanträge unterliegen der Verifizierung durch Symantec gemäß den anwendbaren Bestimmungen dieses Service Level Agreement.

1.3. Dieses Service Level Agreement hat keine Wirkung: (i) zu Zeiten geplanter Wartung oder von Notfallwartung, Zeiten von Nichtverfügbarkeit aufgrund höherer Gewalt oder Handlungen oder Unterlassungen vonseiten entweder des Kunden oder eines Dritten; (ii) während einer von Symantec veranlassten Aussetzung des Service gemäß den Bedingungen der Vereinbarung oder (iii) wenn der Kunde gegen die Vereinbarung verstoßen hat (einschließlich und ohne Einschränkung bei Zahlungsrückstand des Kunden) oder (iv) wenn der Kunde den Service nicht vereinbarungsgemäß konfiguriert hat.

1.4. Die in diesem Service Level Agreement beschriebenen Rechtsmittel stellen das einzige Rechtsmittel dar, das dem Kunden nach dem Vertragsrecht, nach dem Recht der unerlaubten Handlungen (einschließlich, aber nicht beschränkt auf Fahrlässigkeit) oder anderweitig zur Verfügung steht.

1.5. Die kumulative Höchsthaftung von Symantec unter diesem Service Level Agreement in einem Kalendermonat beläuft sich auf nicht mehr als einhundert Prozent (100 %) der vom Kunden für den/die betroffene(n) Service(s) zu zahlenden monatlichen Gebühr.

1.6. Sofern der betroffene Service Teil eines nicht aufteilbaren Servicepakets ist:

- a) Zum Zweck der Berechnung von Servicegutschriften wird die monatliche Gebühr für den betroffenen Service berechnet, indem die Gesamtmonatsgebühr für das nicht aufteilbare Servicepaket durch die Anzahl der in diesem Paket enthaltenen einzelnen Services dividiert wird.
- b) Wenn der Kunde den betroffenen Service gemäß dem vorliegenden Service Level Agreement kündigt, wird die geänderte Gebühr für das nicht aufteilbare Servicepaket berechnet, indem die Gesamtmonatsgebühr für das nicht aufteilbare Servicepaket durch die ursprüngliche Anzahl der in diesem Paket enthaltenen einzelnen Services dividiert und mit der Anzahl der verbleibenden in diesem Paket enthaltenen einzelnen Services multipliziert wird.

2. Ausnahmen bei einem Service Level Agreement für Email Security Services und Web Services.

2.1. Dieses Service Level Agreement hat keine Wirkung: (i) in Bezug auf jegliche E-Mails, die nicht über den Service weitergeleitet wurden (einschließlich, aber nicht beschränkt auf Fälle, in denen der Kunde nicht die erforderlichen Maßnahmen ergriffen hat, um sicherzustellen, dass ausschließlich eingehende E-Mails aus der Symantec-Infrastruktur akzeptiert werden), (ii) oder in Bezug auf jegliche eingehenden oder ausgehenden E-Mails, die ursprünglich an Symantec gesendet wurden und die pro SMTP-Sitzung mehr als 500 Empfänger enthalten.

2.2. Die Service Level für die Email Security Services gelten nicht für den Email Continuity.cloud Service. Folglich sind die Service Level für die Email Security Services in den Absätzen 3 bis 5 unten während jeglicher Zeiträume auszusetzen, in denen sich der Email Continuity.cloud Service in einem aktivierten Zustand befindet.

3. 100 % Serviceverfügbarkeit

3.1. Dieser Service Level für Serviceverfügbarkeit hat nur Wirkung, wenn der Kunde einen oder mehrere der Email Security Services oder Web Services in Anspruch nimmt.

3.2. Im Hinblick auf Email Security Services bezeichnet dieser Service Level für Serviceverfügbarkeit die Möglichkeit zum Aufbau einer SMTP-Sitzung an Port 25 des ausgewiesenen Tower-Clusters gemäß Messung durch den Symantec Tracker. Dieser Service Level gilt nur, wenn der ausgewiesene Tower-Cluster zu Folgendem in der Lage ist:

- a) Empfangen der eingehenden E-Mails des Kunden im Auftrag der Domäne des Kunden rund um die Uhr an sieben Tagen der Woche und
- b) Annehmen der ausgehenden E-Mails des Kunden von einem ordnungsgemäß konfigurierten SMTP-Host des Kunden im Auftrag der Domäne(n) des Kunden rund um die Uhr an sieben Tagen der Woche

3.3. In Bezug auf die Web Services bezeichnet dieser Service Level der Serviceverfügbarkeit die Verfügbarkeit der Web Services zur Annahme der ausgehenden Web-Anforderungen des Kunden und gilt nur, wenn der Host, die Gateway-Geräte oder der/die Proxy(s) des Kunden rund um die Uhr ordnungsgemäß konfiguriert sind.

3.4. Falls die Serviceverfügbarkeit in einem Kalendermonat unter einhundert Prozent (100 %) liegt, kann der Kunde einen Gutschriftenantrag einreichen und erhält ggf. eine Servicegutschrift für die folgende prozentuale Gutschrift:

Prozentuale Serviceverfügbarkeit pro Kalendermonat	Prozentuale Gutschrift der monatlichen Gebühr
< 100 % aber $\geq 99,0$ %	25
< 99 % aber $\geq 98,0$ %	50
< 98,0 %	100 und Kündigung des betroffenen Service im Ermessen des Kunden

3.5. Falls die Serviceverfügbarkeit in einem Kalendermonat unter achtundneunzig Prozent (98 %) fällt, ist der Kunde zur sofortigen Kündigung des betroffenen Service berechtigt sowie zu einer anteilmäßigen Rückerstattung von im Voraus für den betroffenen Service für die Zeit nach der Kündigung bezahlten Gebühren.

4. 100 % E-Mail-Zustellung

4.1. Dieser Service Level für E-Mail-Zustellung hat nur Wirkung, wenn der Kunde einen oder mehrere Email Security Services in Anspruch nimmt.

4.2. Symantec stellt 100 % aller an den oder vom Kunden gesendeten E-Mails vorbehaltlich folgender Bestimmungen zu:

- a) Die E-Mail muss vom ausgewiesenen Tower-Cluster des Kunden empfangen worden sein.
- b) Die E-Mail darf keine Viren, unerwünschte Massen-E-Mails (Spam) oder sonstige Inhalte enthalten, die dazu geführt haben, dass sie durch die Email Security Services abgefangen wurde.

4.3. Falls Symantec vorbehaltlich der Absätze 4.1 und 4.2 oben eine E-Mail an den oder vom Kunden nicht zustellt und der Kunde nicht gegen die Bedingungen des Vertrags verstößt, hat der Kunde mittels einer innerhalb von dreißig (30) Tagen zu übersendenden schriftlichen Benachrichtigung Anspruch auf eine Kündigung der Email Security Services.

5. E-Mail-Latenz – 60 Sekunden

5.1. In Abhängigkeit von Absatz 5.2 hat dieser Service Level für die E-Mail-Latenz nur Wirkung, wenn der Kunde einen oder mehrere Email Security Services in Anspruch nimmt.

5.2. Der Service Level für die E-Mail-Latenz ist nicht auf den Policy Based Encryption Service anwendbar.

5.3. Wenn in einem Kalendermonat die durchschnittliche Gesamtübertragungsdauer (Average Roundtrip Time) (nach Messung durch den Symantec Tracker) für E-Mails, die alle fünf Minuten von und zu jedem Tower für Email Security Services innerhalb des ausgewiesenen Tower-Clusters des Kunden gesendet werden, die in der nachfolgenden Tabelle genannten Verzögerungen überschreitet, kann der Kunde einen Gutschriftenantrag einreichen und erhält gegebenenfalls eine Servicegutschrift gemäß der folgenden Tabelle:

Durchschnittliche Gesamtübertragungsdauer von 100 % der Messungen (in Minuten und Sekunden)	Prozentuale Gutschrift der monatlichen Gebühr
> 1 Min aber ≤ 1 Min 30 Sek	25
> 1 Min 30 Sek aber ≤ 2 Min	50
> 2 Min aber ≤ 2 Min 30 Sek	75
> 2 Min 30 Sek	100

5.4. Dieser Service Level für die E-Mail-Latenz hat keine Wirkung:

- a) Wenn der Kunde Symantec keine Liste einzelner E-Mail-Adressen, auf die der Service anzuwenden ist ("Validierungsliste"), zur Verfügung gestellt hat und der Kunde einem Denial-of-Service-Angriff ausgesetzt ist
- b) Während Verzögerungen, die von einer Mailschleife von den/an die Systeme(n) des Kunden verursacht wurden
- c) Wenn der primäre E-Mail-Server des Kunden nicht in der Lage ist, die E-Mail bei der ersten versuchten Zustellung anzunehmen

6. Web-Latenz – 0,1 Sekunden

6.1. Dieser Service Level für Web-Latenz hat nur Wirkung, wenn der Kunde einen oder mehrere Web Services in Anspruch nimmt.

6.2. Dieser Service Level für Web-Latenz ist nur auf Objekte von maximal 1 MB Größe anwendbar.

6.3. Wenn die für den Verlauf eines Kalendermonats berechnete durchschnittliche Scanzeit für Webinhalte, gemessen vom Zeitpunkt des Empfangs der Inhalte durch Symantec bis zum Zeitpunkt des Übertragungsversuchs der Inhalte durch Symantec, weniger als 100 % gemäß der nachfolgenden Tabelle beträgt, kann der Kunde einen Gutschriftenantrag einreichen und erhält gegebenenfalls eine Servicegutschrift gemäß der folgenden Tabelle:

Durchschnittlicher prozentualer Anteil gescannter Webinhalte innerhalb von 100 Millisekunden	Prozentuale Gutschrift der monatlichen Gebühr
< 100 % aber >= 99,0 %	25
< 99 % aber >= 98 %	50
< 98 % aber >= 97 %	75
< 97 %	100 und Kündigung des betroffenen Service im Ermessen des Kunden

7. Spam – False Positives 0,0003 %

7.1. Dieser Service Level für Spam False Positives (Spam-Fehlmeldungen) hat nur Wirkung, wenn der Kunde den Email AntiSpam.Cloud Service in Anspruch nimmt und die von Symantec empfohlenen Spam-Einstellungen (Symantec Spam Recommended Settings) implementiert. Ferner gilt dieser Service Level nur für eingehende E-Mails.

7.2. Wenn die durchschnittliche Erfassungsrate für Spam False Positives in einem Kalendermonat 0,0003 % des gesamten E-Mail-Verkehrs des Kunden überschreitet, kann der Kunde einen Gutschriftenantrag einreichen und erhält gegebenenfalls eine Servicegutschrift gemäß der folgenden Tabelle:

Erfassungsrate in Prozent für Spam False Positives pro Kalendermonat	Prozentuale Gutschrift der monatlichen Gebühr
> 0,0003 aber <= 0,003	25
> 0,03 aber <= 0,3	50
> 0,03 aber <= 0,3	75
> 0,3	100

7.3. Folgende E-Mails stellen für die Zwecke dieses Service Level keine E-Mails in der Kategorie "Spam False Positive" dar:

- E-Mails, die keine legitimen Geschäfts-E-Mails darstellen
- E-Mails mit mehr als 20 Empfängern
- E-Mails, deren Absender auf der Liste blockierter Absender des Kunden steht, einschließlich und ohne Einschränkung vom einzelnen Benutzer definierte Absender, wenn der Kunde Einstellungen auf Benutzerebene aktiviert hat
- E-Mails, die von einem Computer versendet werden, dessen Sicherheit verletzt wurde
- E-Mails, die von einem Computer versendet werden, der auf der Blockierliste eines Dritten steht
- E-Mails, die über mindestens 80 % gleichen Inhalt verfügen
- E-Mails, die von Scans ausgehender E-Mails abgefangen wurden

8. 99 % Spam-Erfassungsrate

8.1. Dieser Service Level für die Spam-Erfassung hat nur Wirkung, wenn der Kunde den Email AntiSpam.cloud Service in Anspruch nimmt und die empfohlenen Spam-Einstellungen implementiert. Die Bestimmungen dieses Service Level entsprechen der während eines Kalendermonats gemessenen Zahl aus der Kategorie "Spam False Negative". Ferner gilt dieser Service Level nur für eingehende E-Mails.

8.2. Wenn Symantec die Spam-Erfassungsrate in einem Kalendermonat nicht erreicht hat, kann der Kunde einen Gutschriftenantrag einreichen und erhält gegebenenfalls eine Servicegutschrift gemäß der folgenden Tabelle:

Spam-Erfassungsrate in Prozent pro Kalendermonat	Prozentuale Gutschrift der monatlichen Gebühr
> 98 % - <= 99 %	25
> 97 % - <= 98 %	50

> 96 % - <= 97 %	75
< 96 %	100

8.3. Dieser Service Level für die Spam-Erfassung hat keine Wirkung, wenn die E-Mail nicht an eine legitime Adresse gesendet wurde.

8.4. Eine geringere Spam-Erfassungsrate von 95 % gilt für E-Mails, die mehr als 50 % Doppelbyte-Zeichensätze enthalten. Falls diese Spam-Erfassungsrate unter 95 % fällt, hat der Kunde Anspruch auf eine Servicegutschrift von 25 % der monatlichen Gebühr. Falls die Spam-Erfassungsrate unter 90 % fällt, hat der Kunde Anspruch auf eine Servicegutschrift, die 100 % der monatlichen Gebühr entspricht.

9. Spam Service-Gutschriftenanträge

9.1. Damit der Kunde zu Gutschriften gemäß den Absätzen 7 und 8 berechtigt ist, muss er mutmaßliche E-Mails der Kategorie "Spam False Positive" oder "Spam False Negative" innerhalb von 5 Tagen ab Erhalt der E-Mail an support.cloud@symantec.com senden. Symantec ermittelt und bestätigt, ob die E-Mail in die Kategorie "Spam False Positive" oder "Spam False Negative" fällt oder nicht, und zeichnet das Ergebnis auf. Wenn der Kunde meint, Anspruch auf eine Servicegutschrift zu haben, muss er am Ende des Kalendermonats einen Gutschriftenantrag einreichen.

10. E-Mail-Virenschutz – 100 % bekannte und unbekannte Viren

10.1. Dieser Service Level für E-Mail-Virenschutz gilt nur, wenn der Kunde den Email AntiVirus.cloud Service in Anspruch nimmt.

10.2. Falls die Systeme des Kunden in einem Kalendermonat von einem bzw. mehreren bekannten oder unbekannten Viren, die in einer über den Email AntiVirus.cloud Service weitergeleiteten E-Mail enthalten sind, infiziert werden, hat der Kunde Anspruch auf eine Servicegutschrift in Höhe der unten genannten Beträge. Der Kunde muss Symantec dies mittels einer protokollierten und für gültig erklärten Supportanfrage, die bestätigt, dass ein Virus durch den Email AntiVirus.cloud Service an den Kunden weitergegeben wurde, mitteilen. Der Kunde muss einen Gutschriftenantrag einreichen. Wird der Gutschriftenantrag genehmigt, erhält er eine Servicegutschrift, die 100 % der monatlichen Gebühr oder zehntausend US-Dollar/fünftausend Pfund Sterling/zehntausend Euro (10.000 \$/5.000 £/10.000 €) entspricht (abhängig davon, in welcher Währung die Rechnungsstellung des Kunden erfolgt), je nachdem, welcher Betrag geringer ist. Das in diesem Absatz beschriebene Rechtsmittel ist das einzige Rechtsmittel nach dem Vertragsrecht, nach dem Recht der unerlaubten Handlungen (einschließlich und ohne Einschränkung Fahrlässigkeit) oder anderweitig bezüglich einer Infizierung durch einen an den Kunden oder einen Dritten über den Service weitergegebenen Virus. Um Missverständnisse auszuschließen: Das in diesem Absatz beschriebene Rechtsmittel gilt nicht in Fällen vorsätzlicher Selbstinfizierung.

10.3. Die Systeme des Kunden gelten als infiziert, wenn ein Virus, der in einer über den Email AntiVirus.cloud Service empfangenen E-Mail enthalten ist, in den Systemen des Kunden aktiviert wurde, sei es automatisch oder durch manuellen Eingriff.

10.4. Falls Symantec eine vireninferierte E-Mail erkennt, aber nicht aufhält, benachrichtigt Symantec die jeweiligen Supportansprechpartner des Kunden umgehend und stellt ausreichende Informationen zur Verfügung, die den Kunden dazu befähigen, die vireninferierte E-Mail zu identifizieren und zu löschen. Wenn eine solche Benachrichtigung zur Abwendung der Infizierung führt, ist das oben beschriebene Rechtsmittel nicht anwendbar. Falls der Kunde nicht umgehend auf die Benachrichtigung von Symantec reagiert, ist das oben beschriebene Rechtsmittel nicht anwendbar.

10.5. Der Email AntiVirus.cloud Service scannt die E-Mail und ihre Anhänge im größtmöglichen Umfang. Es ist eventuell nicht möglich, Anhänge mit Inhalt zu scannen, der direkt vom Absender kontrolliert wird (z. B. kennwortgeschützte und/oder verschlüsselte Anhänge). Derartige E-Mails und/oder Anhänge sind vom Service Level ausgeschlossen und das oben beschriebene Rechtsmittel ist nicht anwendbar.

10.6. Dieser Service Level für den E-Mail-Virenschutz hat keine Wirkung in Bezug auf Viren, die vom Kunden absichtlich verbreitet wurden.

10.7. Dieser Service Level für den E-Mail-Virenschutz hat keine Wirkung in Bezug auf andere Arten von Malware, einschließlich aber nicht beschränkt auf Trojaner, Phishing, Spyware, Adware oder Links zu Websites, die bösartigen Content enthalten.

11. E-Mail-Virusfehlmeldungen – 0,0001 %

11.1. Dieser Service Level für E-Mail-Virusfehlmeldungen hat nur Wirkung, wenn der Kunde den Email AntiVirus.cloud Service in Anspruch nimmt.

11.2. Wenn die Erfassungsrate für E-Mail-Virusfehlmeldungen in einem Kalendermonat 0,0001 % des gesamten E-Mail-Verkehrs des Kunden überschreitet, kann der Kunde einen Gutschriftenantrag einreichen und erhält gegebenenfalls eine Servicegutschrift gemäß der folgenden Tabelle:

Erfassungsrate in Prozent für E-Mail-	Prozentuale Gutschrift der
---------------------------------------	----------------------------

Virusfehlmeldungen pro Kalendermonat	monatlichen Gebühr
> 0,0001 aber <= 0,001	25
> 0,001 aber <= 0,01	50
> 0,01 aber <= 0,1	75
> 0,1	100

12. Web-Virenschutz – 100 % Bekannte Viren

12.1. Dieser Service Level für Web-Virenschutz hat nur Wirkung, wenn der Kunde den Web v2 Protect.cloud Service in Anspruch nimmt.

12.2. Falls die Systeme des Kunden in einem Kalendermonat von einem bzw. mehreren bekannten Viren, die in einer über den Web v2 Protect.cloud Service weitergeleiteten URL enthalten sind, infiziert werden, hat der Kunde Anspruch auf eine Servicegutschrift in Höhe der unten genannten Beträge. Der Kunde muss Symantec dies mittels einer protokollierten und für gültig erklärten Supportanfrage (einschließlich Details der URL, von der das Element heruntergeladen wurde), die bestätigt, dass ein bekannter Virus durch den Web v2 Protect.cloud Service an den Kunden weitergegeben wurde, mitteilen. Der Kunde muss einen Gutschriftenantrag einreichen. Wird der Gutschriftenantrag genehmigt, erhält er eine Servicegutschrift, die 100 % der monatlichen Gebühr oder zehntausend US-Dollar/fünftausend Pfund Sterling/zehntausend Euro (10.000 \$/5.000 £/10.000 €) entspricht (abhängig davon, in welcher Währung die Rechnungsstellung des Kunden erfolgt), je nachdem, welcher Betrag geringer ist. Das in diesem Absatz beschriebene Rechtsmittel stellt das einzige Rechtsmittel dar, das dem Kunden nach dem Vertragsrecht, nach dem Recht der unerlaubten Handlungen (einschließlich, aber nicht beschränkt auf Fahrlässigkeit) oder anderweitig zur Verfügung steht. Um Missverständnisse auszuschließen: Das in diesem Absatz beschriebene Rechtsmittel gilt nicht in Fällen vorsätzlicher Selbstinfizierung oder bei vorsätzlichem Herunterladen von bekanntermaßen bösartigem Code durch den Kunden.

12.3. Die Systeme des Kunden gelten als infiziert, wenn ein bekannter Virus, der in einer über den Web v2 Protect.cloud empfangenen Web-Transaktion enthalten ist, in den Systemen des Kunden aktiviert wurde, sei es automatisch oder durch manuellen Eingriff.

12.4. Falls Symantec einen bekannten Virus als Teil einer URL, die über den Symantec Web v2 Protect.cloud Service weitergeleitet wurde, erkennt, aber nicht aufhält, benachrichtigt Symantec den Kunden umgehend und stellt ausreichende Informationen zur Verfügung, die den Kunden dazu befähigen, das Element zu identifizieren und zu löschen. Wenn eine solche Benachrichtigung zur Abwendung der Infizierung führt, ist das im Absatz oben beschriebene Rechtsmittel nicht anwendbar. Falls der Kunde nicht umgehend auf die Benachrichtigung von Symantec reagiert, ist das oben beschriebene Rechtsmittel nicht anwendbar.

12.5. Der Web v2 Protect.cloud Service scannt das heruntergeladene Webelement im größtmöglichen Umfang. Es ist unter Umständen nicht möglich, Elemente zu scannen, die zu Kommunikationszwecken über die unterstützten Webprotokolle (HTTP und FTP über HTTP) verkapselt oder getunnelt sind, mittels HTTPS befördert werden, aus ihrer ursprünglichen Form für Verbreitung, Produktlizenzschutz, Download oder Update komprimiert oder verändert wurden, oder die Inhalt umfassen, der direkt vom Absender kontrolliert wird (zum Beispiel kennwortgeschützte und/oder verschlüsselte Elemente). Derartige Elemente und/oder Anhänge sind vom Service Level ausgeschlossen und das oben beschriebene Rechtsmittel ist nicht anwendbar.

13. Technischer Support und Störungsreaktion rund um die Uhr

13.1. Symantec stellt vierundzwanzig (24) Stunden am Tag an sieben (7) Tagen der Woche folgende Leistungen bereit:

- a) Technischen Support für den Kunden bei Problemen mit dem Service
- b) Kontakt zum Kunden hinsichtlich einer Lösung dieser Probleme

13.2. Immer wenn ein Kunde Symantec gegenüber per Telefon oder E-Mail ein Problem oder eine Störung meldet oder um Serviceinformationen bittet, wird die jeweilige Prioritätsstufe ermittelt, und Symantec reagiert darauf in der in der folgenden Tabelle definierten Weise:

Prioritätsstufe	Beschreibung	Reaktionsziel	Prozentuale Gutschrift der monatlichen Gebühr bei Nichterfüllen der Zielvorgabe

Schwere grad 1	Serviceausfall	Reaktion auf 95 % Anfragen binnen 2 Stunden	15
Schwere grad 2	Teilweiser Verlust des Service oder Servicebeeinträchtigung	Reaktion auf 85 % Anfragen binnen 4 Stunden	10
Schwere grad 3	Möglicherweise den Service beeinflussende oder den Service nicht beeinflussende Informationsanfrage	Reaktion auf 75 % Anfragen binnen 8 Stunden	5

13.3. Auf Handlungen des Kunden zurückzuführende Störungen oder Störungen, die Handlungen vonseiten anderer Serviceanbieter erfordern, unterliegen nicht der Kontrolle von Symantec und sind als solche ausdrücklich vom diesem Service Level ausgeschlossen.

13.4. Vorbehaltlich des Absatzes oben, falls der Kunde der Ansicht ist, dass er eine Verzögerung bei der Reaktion von Symantec auf eine Anfrage (jenseits der in Absatz 13.2 oben definierten Parameter) hinnehmen musste, hat er gegebenenfalls Anspruch auf eine Servicegutschrift gemäß der obigen Tabelle. Gutschriftenanträge müssen die Zeit, das Datum und die Protokollnummer des Vorfalls angeben.

14. Verfügbarkeit des Archiving.cloud (P) Service

14.1. Die Bestimmungen der Absätze 14 und 15 gelten nur für den Archiving.cloud (P) Service.

14.2. Für den Archiving.cloud (P) Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 99,9 % gewährleistet; hiervon ausgeschlossen sind Zeitfenster für geplante Wartungsarbeiten und für Notfallwartungsarbeiten. In diesem Fall bezieht sich "Verfügbarkeit" auf die Bereitschaft der von Symantec gehosteten Infrastruktur zur Annahme und Archivierung von E-Mails. Für die Zwecke der Berechnung der Nichtverfügbarkeit gelten folgende Kriterien: (i) die Messung wird von den Überwachungssystemen von Symantec durchgeführt (diese Messungen können dem Kunden auf schriftliche Anforderung zur Verfügung gestellt werden), (ii) die Überwachung findet in Zeitabständen von fünf (5) Minuten statt, wobei zwei aufeinanderfolgende Fehler erforderlich sind, damit ein Ausfall vorliegt, (iii) nur die von Symantec gehostete Infrastruktur wird einer Messung unterzogen, und diese Messung schließt jegliche Nichtverfügbarkeit infolge eines Ausfalls der E-Mail-Archivierungs-Appliance, eines Ausfalls des Kundennetzwerks oder eines Internetausfalls aus.

14.3. Für jedes eine (1) Prozent (oder eines Teils davon) der Nichtverfügbarkeit, um die das Verfügbarkeitsziel von 99,9 % nach Absatz 14 im fraglichen Kalendermonat verfehlt wird, hat der Kunde Anspruch auf eine Servicegutschrift, die zehn Prozent (10 %) der Symantec in Bezug auf den Service zustehenden monatlichen Gebühr entspricht. Die Höhe der Gutschrift ist pro Kalendermonat auf maximal 100 % der monatlichen Gebühr beschränkt. Der Kunde kann den Archiving.cloud (P) Service nach seinem alleinigen Ermessen kündigen, falls diese Verfügbarkeit in einem Kalendermonat unter neunzig Prozent (90 %) fällt.

15. Archiving.cloud (P) Service – Appliance-Service-Level

15.1. Falls eine E-Mail-Archivierungs-Appliance während der Garantiezeit aus Gründen ausfällt, die von der beschränkten Symantec-Garantie (Symantec Limited Warranty) abgedeckt werden (gemäß Definition in der mit der E-Mail-Archivierungs-Appliance gelieferten Dokumentation), arbeitet Symantec mit dem Kunden zusammen, ohne dass dabei für den Kunden Kosten entstehen, um die Fehler in der E-Mail-Archivierungs-Appliance innerhalb von vier (4) Stunden ab Erhalt der Benachrichtigung über das Problem vom Kunden während der üblichen Geschäftszeiten und innerhalb von acht (8) Stunden ab Erhalt der Benachrichtigung über das Problem außerhalb der üblichen Geschäftszeiten zu beheben. Innerhalb von zwei (2) Tagen nach Erhalt der Benachrichtigung über das Problem führt Symantec eine der folgenden Aktionen durch:

- Benachrichtigt den Kunden, dass die E-Mail-Archivierungs-Appliance ordnungsgemäß funktioniert und dass das Problem nicht auf die E-Mail-Archivierungs-Appliance oder die Software zurückzuführen ist
- Repariert die E-Mail-Archivierungs-Appliance mittels Hardware und/oder Software
- Setzt den Kunden davon in Kenntnis, dass die E-Mail-Archivierungs-Appliance ersetzt werden muss

- d) Falls Symantec nicht in der Lage ist, die E-Mail-Archivierungs-Appliance zu reparieren oder zu ersetzen, wird die monatlichen Gebühr für den Archiving.cloud (P) Service für die aktuelle Laufzeit zurückerstattet und der Archiving.cloud (P) Service wird beendet

15.2. Sollte Symantec unter Absatz 15.1.c. zur Bereitstellung eines Ersatzes für die E-Mail-Archivierungs-Appliance verpflichtet sein, hat Symantec die Ersatz-Appliance innerhalb von vier (4) Werktagen ab dem Zeitpunkt der Benachrichtigung des Kunden hinsichtlich der Notwendigkeit einer neuen E-Mail-Archivierungs-Appliance an den Standort des Kunden zu liefern.

15.3. Sollte Symantec gemäß den Absätzen 15.1.b. und 15.1.c. oben zur Reparatur oder Ersetzung der E-Mail-Archivierungs-Appliance oder Software verpflichtet sein und versäumt es, dies in den in Absätzen 15.1. und 15.2. festgelegten zeitlichen Rahmen zu tun, erstattet Symantec dem Kunden fünf Prozent (5 %) der monatlichen Gebühr für den Service für jeden versäumten Tag nach diesem zeitlichen Rahmen zurück, bis zu einem Höchstsatz von 100 % der monatlichen Gebühr.

15.4. Die in diesem Absatz 15 beschriebenen Bestimmungen stellen das einzige Rechtsmittel des Kunden in Bezug auf Mängel oder Verletzungen der Garantie in Bezug auf die E-Mail-Archivierungs-Appliance dar.

16. Email Continuity.cloud Service

16.1. Die Bestimmungen des vorliegenden Absatzes 16 gelten ausschließlich für den Email Continuity.cloud Service.

16.2. Für den Email Continuity.cloud Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 99,9 % gewährleistet; hiervon ausgeschlossen sind Zeitfenster für geplante Wartungsarbeiten und Notfallwartungsarbeiten. In diesem Fall bezieht sich "Verfügbarkeit" auf die Bereitschaft der von Symantec gehosteten Infrastruktur zur Synchronisierung wichtiger System- und Benutzerdaten. Für die Zwecke der Berechnung der Nichtverfügbarkeit gelten folgende Kriterien: (i) Die Messung erfolgt durch die Symantec-Überwachungssysteme (diese Messung kann dem Kunden auf schriftliche Anfrage vorgelegt werden), und (ii) die Messung bezieht sich ausschließlich auf die von Symantec gehostete Infrastruktur und schließt jegliche Nichtverfügbarkeit aus, die aufgrund eines Netzwerkausfalls auf Seiten des Kunden, eines Ausfalls seitens einer Drittpartei oder eines DNS-Problems, das sich der direkten Kontrolle durch Symantec entzieht, verursacht wird.

16.3. Für jedes eine (1) Prozent (oder eines Teils davon) der Nichtverfügbarkeit, um die das Verfügbarkeitsziel von 99,9 % nach dem vorliegenden Absatz 16.1 im fraglichen Kalendermonat verfehlt wird, hat der Kunde Anspruch auf eine Gutschrift, die zehn Prozent (10 %) der Symantec in Bezug auf den Email Continuity.cloud Service zustehenden monatlichen Gebühr entspricht. Die Höhe der Gutschrift ist pro Kalendermonat auf maximal 100 % der monatlichen Gebühr für den Service beschränkt. Der Kunde kann den Email Continuity.cloud Service nach seinem alleinigen Ermessen kündigen, falls diese Verfügbarkeit in einem Kalendermonat unter neunzig Prozent (90 %) fällt.

17. Symantec Email Continuity Archive.cloud oder Symantec Email Continuity Archive Lite.cloud Service

17.1. Die Bestimmungen des vorliegenden Absatzes 17 gelten ausschließlich für den Symantec Email Continuity Archive.cloud Service und den Symantec Email Continuity Archive Lite.cloud Service.

17.2. Für den Symantec Email Continuity Archive.cloud Service und den Symantec Email Continuity Archive Lite.cloud Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 99,95 % gewährleistet. Die Verfügbarkeit wird berechnet, indem die Gesamtzahl der Stunden, in denen der Symantec Email Continuity Archive.cloud Service bzw. der Symantec Email Continuity Archive Lite.cloud Service (wie zutreffend) nicht verfügbar war (wobei Zeiten mit kundenseitigen Netzwerkausfällen, Wartungszeiten oder Zeiten mit DNS-Problemen, die nicht der direkten Kontrolle von Symantec unterliegen, nicht berücksichtigt werden) durch die Gesamtzahl der geplanten verfügbaren Stunden des Symantec Email Continuity Archive.cloud Service bzw. des Symantec Email Continuity Archive Lite.cloud Service (wie zutreffend) im betreffenden Kalendermonat dividiert wird.

17.3. Für jedes eine (1) Prozent Nichtverfügbarkeit jenseits der Verfügbarkeitsvorgabe von 99,95 % gemäß diesem Absatz 16 im betreffenden Kalendermonat hat der Kunde Anspruch auf eine Servicegutschrift, deren Höhe den Gebühren entspricht, die bezüglich des Symantec Email Continuity Archive.cloud Service bzw. des Symantec Email Continuity Archive Lite.cloud Service (wie zutreffend) für einen (1) Kalendertag, an dem der Symantec Email Continuity Archive.cloud Service bzw. der Symantec Email Continuity Archive Lite.cloud Service bereitgestellt wurde, an Symantec gezahlt wurden.

18. Symantec Enterprise Vault.cloud Service oder AdvisorMail on Symantec.cloud Service

18.1. Die Bestimmungen des vorliegenden Absatzes 17 gelten für Symantec Enterprise Vault.cloud Service und AdvisorMail on Symantec.cloud Service.

18.2. Symantec gewährleistet 99,99 % Verfügbarkeit für den Symantec Enterprise Vault.cloud Service und AdvisorMail on Symantec.cloud Service. Wenn die Verfügbarkeit in einem Kalendermonat unter 99,99 % sinkt, hat der Kunde in Abhängigkeit von Absatz 18.3 unten Anspruch auf eine Servicegutschrift gemäß der folgenden Tabelle.

Verfügbarkeit	Prozentuale Gutschrift der
---------------	----------------------------

	monatlichen Gebühr
< 99,99 % aber ≥ 99,9 %	5 % der Monatsgebühr
< 99,9 % aber ≥ 98,0 %	10 % der Monatsgebühr
< 98,0 % aber ≥ 95,0 %	15 % der Monatsgebühr
< 95,0 % aber ≥ 89,9 %	25 % der Monatsgebühr
< 89,9 %	2,5 % der monatlichen Gebühr für jedes Prozent (1 %) nicht geleisteter Verfügbarkeit bis maximal 100 % der monatlichen Gebühr

18.3. Gutschriftenanträge müssen Datums- und Uhrzeitangaben zu den Zeiten von Nichtverfügbarkeit enthalten. Symantec vergleicht die Angaben des Kunden mit den von Symantec erfassten Überwachungsdaten zur Verfügbarkeit. In Reaktion auf einen Gutschriftenantrag wird eine Servicegutschrift ausgestellt, wenn aufgrund der Nichtverfügbarkeit die Ausgabe einer Gutschrift gemäß der oben in Absatz 18.2 aufgeführten Tabelle veranlasst wird. Die im vorliegenden Absatz 18.3 beschriebene Servicegutschrift ist das einzige und ausschließliche Rechtsmittel des Kunden in Verbindung mit einer etwaigen Nichtverfügbarkeit. Nichtverfügbarkeit zu Zeiten geplanter Wartung oder von Notfallwartung ist von den Verfügbarkeitsberechnungen ausgeschlossen.

19. Symantec Web Security Archiving.cloud

19.1. Die Bestimmungen des vorliegenden Absatzes 19 gelten nur für den Symantec Web Security Archiving.cloud Premium Service.

19.2. Für den Symantec Web Security Archiving.cloud Premium Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 99,9 % gewährleistet. Die Verfügbarkeit wird berechnet, indem die Gesamtzahl der Stunden, in denen der Symantec Web Security Archiving.cloud Premium Service nicht verfügbar war (wobei Zeiten mit kundenseitigen Netzwerkausfällen, Wartungszeiten oder Zeiten mit anderen Problemen, die nicht der direkten Kontrolle von Symantec unterliegen, nicht berücksichtigt werden) durch die Gesamtzahl der geplanten verfügbaren Stunden des Symantec Web Security Archiving.cloud Premium Service im betreffenden Kalendermonat dividiert wird.

19.3. Für jedes eine (1) Prozent (oder eines Teils davon) der Nichtverfügbarkeit unterhalb des Verfügbarkeitsziels von 99,9 % unter dem vorliegenden Absatz 19.3 im betroffenen Kalendermonat hat der Kunde Anspruch auf eine Gutschrift in Höhe von zehn Prozent (10 %) der monatlich an Symantec im Zusammenhang mit dem Symantec Web Security Archiving.cloud Premium Service zu zahlenden Gebühr. Die Höhe der Gutschrift ist pro Kalendermonat auf maximal 100 % der monatlichen Gebühr beschränkt. Der Kunde kann den Symantec Web Security Archiving.cloud Service nach eigenem Ermessen jederzeit kündigen, wenn diese Verfügbarkeit in einem Kalendermonat weniger als 90 % beträgt.

19.4. Die in Absatz 19.3 beschriebene Servicegutschrift ist das einzige und ausschließliche Rechtsmittel des Kunden in Verbindung mit einer etwaigen Nichtverfügbarkeit des Service.

20. Symantec Endpoint Protection Small Business Edition 2013

20.1. Die Bestimmungen unter dem vorliegenden Absatz 20 gelten ausschließlich für den Symantec Endpoint Protection Small Business Edition 2013 Service.

20.2. Für den Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 100 % gewährleistet; hiervon ausgeschlossen sind Zeitfenster für geplante Wartungsarbeiten und Notfallwartungsarbeiten. In diesem Fall bezieht sich "Verfügbarkeit" auf die Bereitschaft der von Symantec gehosteten Infrastruktur für die Synchronisierung von Richtlinieninformationen. Für die Zwecke der Berechnung der Nichtverfügbarkeit gelten folgende Kriterien: (i) Die Messung erfolgt durch die Symantec-Überwachungssysteme (diese Messung kann dem Kunden auf schriftliche Anfrage vorgelegt werden), und (ii) die Messung bezieht sich ausschließlich auf die von Symantec gehostete Infrastruktur und schließt jegliche Nichtverfügbarkeit aus, die aufgrund eines Netzwerkausfalls auf Seiten des Kunden, eines Ausfalls seitens einer Drittpartei oder eines DNS-Problems, das sich der direkten Kontrolle durch Symantec entzieht, verursacht wird.

20.3. Für jedes eine (1) Prozent (oder eines Teils davon) der Nichtverfügbarkeit unterhalb des Verfügbarkeitsziels von 100 % unter dem vorliegenden Absatz 20.3 im fraglichen Kalendermonat hat der Kunde Anspruch auf eine Servicegutschrift, die zehn Prozent (10 %) der Symantec in Bezug auf den Service zustehenden monatlichen Gebühr

entspricht. Die Höhe der Gutschrift ist pro Kalendermonat auf maximal 100 % der monatlichen Gebühr beschränkt. Der Kunde kann den Service nach seinem alleinigen Ermessen kündigen, falls diese Verfügbarkeit zu irgendeinem Zeitpunkt in einem Kalendermonat unter neunzig Prozent (90%) fällt.

20.4. Die in diesem Absatz 20.3 beschriebene Servicegutschrift ist das einzige und ausschließliche Rechtsmittel des Kunden in Verbindung mit einer etwaigen Nichtverfügbarkeit des Service.

21. Symantec Backup Exec.cloud

21.1. Die Bestimmungen dieses Absatzes 21 gelten ausschließlich für den Symantec Backup Exec.cloud Service.

21.2. Für den Symantec Backup Exec.cloud Service wird pro Kalendermonat jeweils eine Verfügbarkeit von 100 % gewährleistet; hiervon ausgeschlossen sind Zeitfenster für geplante Wartungsarbeiten und Notfallwartungsarbeiten. In diesem Fall bezieht sich "Verfügbarkeit" auf die Bereitschaft der von Symantec gehosteten Infrastruktur für die Synchronisierung von Richtlinieninformationen. Für die Zwecke der Berechnung der Nichtverfügbarkeit gelten folgende Kriterien:

- a) Die Messung wird von den Überwachungssystemen von Symantec durchgeführt (diese Messungen können dem Kunden auf schriftliche Anforderung zur Verfügung gestellt werden).
- b) Die Messung bezieht sich ausschließlich auf die von Symantec gehostete Infrastruktur und schließt jegliche Nichtverfügbarkeit aus, die aufgrund eines Netzwerkausfalls auf Seiten des Kunden, eines Ausfalls seitens einer Drittpartei oder eines DNS-Problems, das sich der direkten Kontrolle durch Symantec entzieht, verursacht wird.

21.3. Für jedes eine (1) Prozent (oder eines Teils davon) der Nichtverfügbarkeit unterhalb des Verfügbarkeitsziels unter diesem Absatz 21.3 im fraglichen Kalendermonat hat der Kunde Anspruch auf eine Servicegutschrift, die zehn Prozent (10 %) der Symantec in Bezug auf den Service zustehenden monatlichen Gebühr entspricht. Die Höhe der Gutschrift ist pro Kalendermonat auf maximal 100 % der monatlichen Gebühr beschränkt. Der Kunde kann den Symantec Backup Exec.cloud Service nach eigenem Ermessen jederzeit kündigen, wenn diese Verfügbarkeit in einem Kalendermonat weniger als neunzig Prozent (90 %) beträgt. Die im vorliegenden Absatz 21.3 beschriebene Servicegutschrift ist das einzige und ausschließliche Rechtsmittel des Kunden in Verbindung mit einer etwaigen Nichtverfügbarkeit des Symantec Backup Exec.cloud Service.

ENDE DER ANLAGEN